(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 330 404 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication of patent specification : **30.11.94 Bulletin 94/48**

(51) Int. Cl.[5] : **G07F 7/10,** G06K 19/06

(21) Application number : **89301626.1**

(22) Date of filing : **20.02.89**

(54) Integrated circuit cards.

(30) Priority : **20.02.88 JP 38078/88**
22.06.88 JP 154014/88

(43) Date of publication of application : **30.08.89 Bulletin 89/35**

(45) Publication of the grant of the patent : **30.11.94 Bulletin 94/48**

(84) Designated Contracting States : **DE ES FR GB**

(56) References cited :
EP-A- 0 138 219
EP-A- 0 147 337

(73) Proprietor : **FUJITSU LIMITED**
1015, Kamikodanaka
Nakahara-ku
Kawasaki-shi Kanagawa 211 (JP)

(72) Inventor : **Seki, Junji**
5-8-11, Higashikashiwagaya
Ebina-shi Kanagawa 243-04 (JP)

(74) Representative : **Fane, Christopher Robin King et al**
HASELTINE LAKE & CO.
Hazlitt House
28 Southampton Buildings
Chancery Lane
London, WC2A 1AT (GB)

EP 0 330 404 B1

Description

The present invention relates to integrated circuit cards (hereinafter referred to as IC cards).

The convenience of IC cards for multi-purpose usage, such as for banking, shopping, and travel services, etc., has encouraged a widespread use of these cards, which although having different nomenclatures, for example, Smart Card or Chip-in Card, provide similar facilities.

As explained in detail hereinafter, one form of prior art IC card contains a processor, i.e. a central processing unit (CPU) and a memory, both packaged in a plastic plate as one body. The capacity of the memory might typically be 8K bytes, but such memory capacity may not be sufficient when the facilities provided by the IC card are to be expanded. If a large capacity memory is required a separate optically readable memory may be provided on the card, as disclosed in EP-A-0147337, for example a laser memory as disclosed in EP-A-0138219. A laser memory can be written and read by laser light, similarly to a CD-ROM. The capacity of a laser memory can be several million bytes.

An alternative form of IC card system has been considered, having a magnetic strip thereon, in which information recorded on the magnetic strip is read and handled by a processor separate from the internal processor of the IC card.

In such prior art systems, the internal processor of the card only reads and handles information stored in an internal memory of the card.

According to the present invention there is provided an IC card containing a processor, for communicating with an external card-acceptance device, and an internal memory, connected to cooperate with the processor, for storing data to be accessed by the processor, there being mounted on a surface of the card an external memory for storing further data, which further data is to be accessible only by way of the said external card-acceptance device, characterised in that the said internal memory includes a directory for storing respective addresses at which data files are stored in the external memory, and in that the said processor is provided with an external memory access program for enabling such a card-acceptance device to obtain, from the said directory, address information necessary to enable the card-acceptance device to access such files in the external memory.

In an embodiment of the present invention, the IC card is provided with an internal processor (CPU) which includes communication means for accessing an external auxiliary memory, provided integrally with the body of the IC card, by way of an external card-acceptance device.

An IC card system embodying the present invention desirably provides protection against illegal access to information in the external memory, and can advantageously provide an IC card system in which records relating to past access to information recorded in the external memory (update history) can be easily obtained by an authorised user after verification.

Reference will now be made, by way of example, to the accompanying drawings, in which:

Figure 1 is a perspective view of a conventional IC card;

Figure 2 is a schematic diagram of the internal construction of an integrated circuit module;

Figure 3 is a perspective view of an IC card of a system embodying the present invention;

Figure 4 is a schematic diagram of an arrangement of devices in an IC card of a system embodying the present invention;

Figure 5 is a schematic diagram of the general construction of devices mounted on and in an IC card for a system embodying the present invention;

Fig. 6 is a block diagram of an IC card system embodying of the present invention;

Fig. 7 is a block diagram illustrating the principles of construction of an IC card for a system embodying the present invention;

Fig. 8 is a block diagram for clarifying a write process performed in the IC card shown in Fig. 7;

Fig. 9 is a block diagram for clarifying a read process performed in the IC card shown in Fig. 7;

Figs. 10A and 10B display a general concept of a data processing system,including an IC card, embodying the present invention;

Figs. 11A and 11B are flow charts of a process for each command, performed by a CPU in an IC card of a system embodying the present invention;

Fig. 12 is a detailed flow chart of the process "A" shown in Fig. 11B;

Fig. 13 is a detailed flow chart of the process "B" shown in Fig. 11B;

Fig. 14 is a detailed flow chart of the process "C" shown in Fig. 11B;

Fig. 15 is a detailed flow chart of the process "D" shown in Fig. 11B;

Fig. 16 is a detailed flow chart of the process "E" shown in Fig. 11B;

Fig. 17 is a detailed flow chart of the process "F" shown in Fig. 11B;

Fig. 18 is a detailed flow chart of the process "G" shown in Fig. 11B;

Fig. 19 is a detailed flow chart of the process "H" shown in Fig. 11B;

Fig. 20 is a detailed flow chart of the process "I" shown in Fig. 11B;

Fig. 21 is a detailed flow chart of the process "J" shown in Fig. 11B;

Fig. 22 is a schematic diagram of the general construction of devices mounted in and on an IC

card, particularly a memory history management part, of a system embodying the present invention;

Figs. 23A and 23B show a specific arrangement of the memory history management part shown in Fig. 22; and

Figs. 24A and 24B illustrate a flow chart of read and write operations at an external memory (EMEM), and show an arrangement of related memories.

Figure 1 is a perspective view of a conventional IC card. In Fig. 1, reference 1 represents an IC card. The IC card 1 contains an integrated circuit module 2 comprising a processor (CPU) and an internal memory (neither of which are shown). The CPU and the memory transmit and receive data to and from an external card-acceptance device via a plurality of contacts 3. Fig. 1 shows the rear surface of the IC card; the front surface thereof has a variety of devices mounted thereon, such a display unit, a ten key unit, and so on.

Fig. 2 is a schematic diagram of an internal construction of an integrated circuit module. The main components of the integrated circuit module 2 are the processor (CPU) 4 and the internal memory (IMEM) 5. The (CPU) 4 provides an IC card access means 6 and the memory, generally a main memory, provides a plurality of format areas 8; these format areas 8 also define a file 9.

The internal memory access means (IMAM) 6 sets up an operating system and is able to process an access of the IC card 1 to the external card acceptance device. When the access is directed to the file 9 in the memory 5, a search is first made of a directory 7, which stores file numbers (Nos.).

In Fig. 2, the memory (IMEM) comprises an IC memory, for example, an electronically erasable programmable read only memory (EEPROM). The capacity of the IC memory might typically be 8 K bytes. As previously mentioned, such a memory capacity is not sufficient to develop a versatile general-purpose IC card, and accordingly, in the prior art, a laser memory card may be used as an accessory to the IC card. However, it is inconvenient to utilize a separate laser memory card with an IC card, despite the very large memory capacity of the laser memory card.

In Fig. 3, an IC card of a system embodying the present invention is provided with an external memory 11 mounted on the surface of the body of the IC card 10 to form a monolithic structure. The external memory 11 is adhered to the body of the IC card 10. As such, the external memory 11 is physically and logically separated from an integrated circuit module 12.

Figure 4 is a schematic diagram of an arrangement of devices in an IC card of a system embodying the present invention. The IC card 10 contains the processor (CPU) 4 and the internal memory (IMEM) 5, i.e. a main memory, both incorporated in the integrated circuit module 12, i.e. an IC chip. The contacts (shown by Fig. 3 but not illustrated in Fig. 4) are used for data communication between the processor 4, together with the internal memory 5, and the external IC card acceptance device. The external memory (EMEM) 11 does not perform data communication via the contacts 3, but communicates directly with the external IC card acceptance means, as illustrated by a two-way arrow in Fig. 4. Note, identical components are generally represented by the same reference numerals or characters throughout the drawings.

Figure 5 is a schematic diagram of the general construction of devices mounted on and in an IC card of a system embodying the present invention. The processor (CPU) 4 is provided with a program ROM which includes therein the internal memory access means (IMAM) 6 and external memory access means (EMAM) 23. The means (IMAM) 6 and means (EMAM) 23 are constituted by programs.

The internal memory (IMEM) 5 is preferably a non-volatile memory, such as an EEPROM, and has a first directory 21 and a second directory 22 formed therein. The second directory 22 defines those format areas 8, of the file 9, that are allotted for the internal memory per se (main memory), and thus the second directory 22 is substantially the same as the directory 7 shown in Fig. 2. The first directory 21, however, defines those format areas 8 of the file 9 that are allotted for use in accessing the external memory 11. The format areas 8, and format areas 18 (explained below) in the external memory 11, store user data relating to the IC card owner.

The external memory 11 is composed of a password area 17 and the format areas 18 setting up a file 19. The password in the area 17 is used in an authentication check of the external memory 11 performed by the internal processor.

The external memory (EMEM) 11 can have a memory capacity much larger than that of the internal memory (IMEM) 5, and accordingly, the external memory 11 may be an optical memory, such as a laser memory, which may have a memory capacity of several M bytes even though small in size.

Figure 6 is a block diagram of an IC card system embodying the present invention. In Fig. 6, the characters "CC" denote a conventional communication controller, 20 denotes an external IC card-acceptance device provided with a conventional reader-writer for data communication with the IC card 10, 24 an access unit for accessing the external memory (EMEM) 11 via an interface 27, for example an optical reading and writing device, 26 a processor containing in particular a terminal EMAM, i.e. external memory access means, and 30 a terminal station, for example a personal computer 31 handling an application program (APL).

In Fig. 6, a first logical system constituted by the

CPU 4 and the external memory (EMEM) 11 is isolated from a second logical system constituted by the CPU 4 and the internal memory (MEM) 5, although the first logical system and the second logical system can be logically connected together by the external IC card acceptance means 20 via the respective interfaces (27 and 3). Only data handled by the CPU 4 is sent to the external memory (EMEM) 11, and read and write operations for the external memory are carried out by using only addresses determined by the CPU 4. The CPU 4 executes the card EMAM program, and the IC card acceptance means (EIAM) 20 (e.g. the reader-writer and reading and writing device) communicates with the CPU 4 and the EMEM 11. In the EIAM 20, the processor (CPU) 26 executes a terminal EMAM program. The CPU (terminal EMAM) 26 is supplied with a command by the aforesaid application program (APL), and in accordance with the kind of command, the CPU 26 selectively executes an internal processing of the terminal EMAM, an access to the external memory 11, and an access to the CPU 4 (device EMAM), and according to the result of this internal processing and the result of the access, an appropriate response is returned to a personal computer 31 (application program). The CPU 4 (card EMAM), after recognition by the terminal EMAM 26 of a command from the application program, is called by the terminal EMAM 26, if required by the resultant recognition, and the CPU 4 then executes a command given by the terminal EMAM. The result of this command execution is returned to the terminal EMAM.

When using the IC card 10, security must be taken into consideration, particularly the security of data stored in the external memory (EMEM) 11. Otherwise the contents of the EMEM 11 could be easily stolen by a third party, because the EMEM 11 is exposed outside the body of the IC card 10.

Figure 7 is a block diagram showing the principles of construction of an IC card of a system embodying the invention. The IC card of Fig. 7 is designed to take security into consideration. In Fig. 7, the IC card 10 having a security function is comprised of the aforesaid external memory (EMEM) 11, an address holding means 44 for holding addresses of the files 19 stored in the EMEM 11, a cryptograph management information memory means 45 for storing the cryptographic management information used for enciphering data and for deciphering the ciphered data, a write processing means 43, a first read processing means 41 and a second read processing means 42. The means 41, 42 and 43 are functions of the CPU 4, and the means 44 and 45 are contained in the internal memory (IMEM) 5, e.g. a main memory.

The write processing means 43 operates upon receipt of a write command WC, and the corresponding write data WD, to encipher the said write data WD with reference to the cryptograph management information, to search for the corresponding address AD of the external memory (EMEM) 11, at which the enciphered write data CWD is to be written, by referring to the address holding means 44, and to send the enciphered write data CWD and the corresponding address AD to the external card-acceptance device 20.

The first read processing means 41 operates upon receipt of a first read command RC1, and the corresponding individual file number FN of the file 19, to search for the corresponding read address RA, related to the given file number, by referring to the address holding means 44, and to send that read address RA to the card-acceptance device 20.

The second read processing means 42 operates upon receipt of a second read command RC2 and a ciphered read data CRD, to decipher the said enciphered read data CRD by referring to the cryptographic management information, and to send the thus deciphered read data DRD to the card-acceptance device 20.

The address holding means 44 is contained in the internal memory, and specifies a new area in the file 9 with reference to a vacant area in the first directory 21.

Note, the means 45 (Fig. 7) has various keys and a ciphering algorithm, commonly known as a "DES" (Data Encryption System proposed by IBM).

Figure 8 is a block diagram for clarifying a write process performed in an IC card of Fig. 7. For example, when writing data in the external memory (EMEM) 11, the following process is carried out:

(I) the given write command WC and the corresponding write data WD are sent to the IC card 10;

(II) the enciphered write data CWD and the corresponding address AD for writing in the external memory (EMEM) 11 are obtained and sent from the IC card 10 to the card acceptance device 20; and

(III) the enciphered write data CWD is written in the EMEM 11.

Figure 9 is a block diagram for clarifying a read process performed in an IC card of Fig. 7. For example, when reading data from the external memory (EMEM) 11, the following process is carried out:

(I) the first read command RC1 and the corresponding individual file number FN are sent to the IC card 10;

(II) the corresponding read address AD for the external memory 11 is found by searching the address holding means 44 and then that address is sent from the IC card 10 to the card-acceptance device 20;

(III) the enciphered read data CRD is obtained, by using the said read address AD, from the external memory 11;

(IV) the enciphered read data CRD from the external memory 11 is sent to the IC card 10 with a second read command RC2; and

(V) deciphered read data DRD is sent from the IC card, in response to the second read command RC2, to the card-acceptance device 28.

Figures 10A and 10B display a general concept of a data processing system including an IC card of a system embodying the invention. Figure 10A shows the IC card 10 and Fig. 10B shows the external IC card acceptance means 20 together with the terminal station 30, e.g. a personal computer. In Fig. 10A, reference numeral 61 denotes a reset processing means, 62 a personal identification number (PIN) verification processing means, 63 a card authentication (AC) processing means, 64 a file open processing means, 65 an E (abbreviation of EMEM 11) write 1 processing means, 66 an E write 2 processing means, 67 an E read 1 processing means, 68 an E read 2 processing means, and 69 a file close processing means. Note, in Fig. 10B, C and R represent a command block and a response block, respectively.

The internal memory 5, e.g. a main memory (IMEM), holds system directory/system information, PIN management information, card issuer identification (ID) management information, card AC management information, APL-ID management information, system AC management information, cryptograph management information, i.e. keys for drafting a cryptograph or deciphering the cryptograph, an EMAM (external memory access means) directory, external memory (EMEM) management files, and so on. The personal identification number (PIN) is a secret code for confirming whether or not the user of the IC card is an entitled user. The PIN is registered in the IC card and, when the IC card is used, the PIN is checked for verification with the secret code input by a user. The IC card is not activated until the PIN verification is satisfied, whereby the IC card is able to access the system (20, 30). A variety of PIN's exist, such as a card manufacturer PIN, a transport PIN, card issuer PIN, an own PIN, and so on. The card issuer ID management information is, for example, a name of a bank, a bank code, a card issuing date, a card issuance number, and so on. The authentication code (AC) is composed of data or an algorithm, in terms of elements (user, card, terminal machine or terminal station, service provider and the like) comprising an IC card system, used for confirming an authentication between any two elements. This data or algorithm is predetermined between two elements, and thereafter, must be kept secret from other parties. Use of the AC enables prevention and detection of non-authorized use or forgery of an IC card and tampering with data in the IC card. The APL-ID is a key essential to a business file when accessed by a business application program. Thus, a business application can be made possible by specifying the APL-ID, to allow access to a required business file without referring to a physical address, and so on. The cryptograph management information produces a cryptograph for deciphering the ciphered data stored in the external memory (EMEM) 11, management information required when new data is to be stored therein, file correspondence numbers of the files in the EMEM 11, a cryptograph for deciphering data which has been cryptographically processed, and so on. The EMAM (external memory access means) directory is composed of a directory for the EMEM 11 and a directory for the internal memory (IMEM) 5. The directory for the EMEM 11 manages file names for managing the EMEM 11, and file correspondence numbers for managing the same. The directory for the IMEM 5 manages a file correspondence number in the external memory (EMEM) 11 and addresses in a memory, managing attribute information with regard to the files in the EMEM 11. The EMEM management serves as an area for managing, in the file units, the attribute information for data in each file of the EMEM 11, which attribute information is managed by the directory for the IMEM. In the data area of the files in the external memory (EMEM) 11, attribute information is recorded which relates to the data in each file of the EMEM 11. Further similar contents to be managed exist, such as the date of drafting of the related files, renewal date, and start and end of each physical address corresponding to the external memory (EMEM) 11.

The EMAM (external memory access means) 23 is provided with the above mentioned processing means 61 to 69 and others. The reset processing means 61 (Fig. 10A) starts operating upon receipt of a RESET command from the means 20/30 (Fig. 10B) and resets the system directory and the system information in the internal memory (IMEM) 5 (Fig. 10A), and then sends a RESET response to the means 20/30. The PIN verification processing means 62 (Fig. 10A) starts operating upon receipt of a PIN verification command accompanied by PIN data and carries out a verification process of the PIN data with reference to the PIN management information (Fig. 10A), and then sends a verification result to the means 20/30. The card AC processing means 63 (Fig. 10A) starts operating upon receipt of a card AC command and performs a check on the card authentication with reference to the card AC management information in the internal memory (IMEM) 5 (Fig. 10A), and then returns the card AC data to the means 20/30. The file open processing means 64 starts operating upon receipt of a file open command and carries out a check of an access right with reference to the system AC management information in the IMEM 5 (Fig. 10A), and then sends the result of the related file open command to the means 20/30. The E write 1 processing means 65 starts operating upon receipt of an E write 1 command and the corresponding data, enciphers the thus given data, and returns the enciphered data and a write position. The above write position is a write position in the external memory

(EMEM) 11, and is obtained by reference to the content of the EMEM management file in the IMEM 5 (Fig. 10A). The E write 2 processing means 66 starts operating upon receipt of an E write 2 command and resultant information (the result of a write operation to the EMEM 11), and writes the result of the write operation to the EMEM 11 for the EMEM management file in the IMEM 5 (Fig. 10A), and then sends the results of the related process to the means 20/30. The E read 1 processing means 67 starts operating upon receipt of the E read 1 command and a file name, and searches for a position in the external memory (EMEM) 11 at which the related file is stored, with reference to the EMEM management file, and then sends the result and the position to the means 20/30 (Fig. 10B). The EMAM read 2 processing means 68 starts operating upon receipt of an E read 2 command and enciphered data and carries out a deciphering operation, with reference to the cryptograph management information in the IMEM 5 (Fig. 10A), and then sends the result and the deciphered data to the means 20/30 (Fig. 10B). The file close processing means 69 starts operating upon receipt of a file close command and carries out a file close operation, and then sends the result to the means 20/30 (Fig. 10B).

When the IC card 10 is inserted into the external IC card acceptance means 20, i.e. the reader-writer, together with the reading and writing device, the terminal means 20/30 (Fig. 10B) sends a RESET command to the IC card 10. Where data is to be written in the external memory (EMEM) 11, the means 20 issues a PIN verification request, a card AC request, a file open request, and a E write 1 request, and thereafter, the related write operation to the EMEM 11 is performed and the E write 2 request is issued. Where data in the EMEM 11 is to be read, the means 20 issues an E read 1 request, and thereafter, the related read operation to the EMEM 11 is carried out. Then an E read 2 request is issued, and when the access to the EMEM 11 is completed, a file close request is issued.

When a PIN verification request is issued, a PIN command is sent to the processor (CPU) 4 forming the processing means 61 through 69; when a card AC request is issued, a card AC command is sent to the CPU 4 in the IC card 10; when a file open request is issued, a file open command is sent to the CPU 4 in the IC card 10; when an E write 1 request is issued, an E write 1 command is sent to the CPU 4 in the IC card 10; when an E write 2 request is issued, an E write 2 command is sent to the CPU 4 in the IC card 10; when an E read 1 request is issued, an E read 1 command is sent to the CPU 4 in the IC card 10; and when an E read 2 request is issued, an E read 2 command is sent to the CPU 4 in the IC card 10.

Figures 11A and 11B are flow charts of a process for each command, performed by a CPU in an IC card of a system embodying the invention. An initial process is started ("a") by a power-ON, and when a command is received ("b") from a PIN PAD (Fig. 10B), a command check is carried out ("c"). If the command code is correct (YES in step "d"), a command parameter check is carried out ("e"). The command parameter check determines whether or not the attribute information conforms with the prescribed parameter. If the result at step "d" is NO, an error response is edited in step "K" in Fig. 11B, and an error response is sent to the means 20 ("L" in Fig. 11B). If the result of the command parameter check is correct (YES in step "f"), a command sequence check is started ("g"). If the result at step "f" is NO, the error response edit is carried out. If the result of the command sequence check is YES ("h"), a command distribution is started ("i"). The command sequence check is introduced to find contradictions in the command sequence; for example, if a file write command precedes a file open command, this is a contradiction. If the result of the command c sequence check is NO in step "h", the flow goes to step "K" (Fig. 11B). When one of the various processes is finished, a response is sent to the means 20 ("L" in Fig. 11B). The above mentioned processes are performed in steps "A" through "J" in Fig. 11B. Note, for brevity, in some of these steps the reference character "E" represents the "EMEM", i.e., the external memory 11 (Fig. 5 and others). Details of these processes will be presented below.

Figure 12 is a detailed flow chart of the process "A" shown in Fig. 11B. In the E OPEN process "A", a double open check is carried out to avoid a double occupation of the same file. If the result is YES, an open finished memo (flag) is made ON (hoist), and a normal response is edited. If the result is NO, an error response is edited.

Figure 13 is a detailed flow chart of the process "B" shown in Fig. 11B. In the E CLOSE process "B", a double close check is carried out for a similar reason as for the double open check, and if the result is YES or NO, a normal or an error response is edited accordingly.

Figure 14 is a detailed flow chart of the process "C" shown in Fig. 11B. In the E WRITE 1 process "C", it is determined whether or not the related data is open. If the result is YES, a data title check is carried out to determine whether or not the related data has a right to access the file. If the result is YES, the corresponding address is found and edited. Further, the corresponding key is found, and using the key, the write data is enciphered, and then edited. Finally, the related edition of the response is performed. If the result of the step (OPEN FINISHED CHECK) is NO, the related edition of the response is performed. This also applies when the result of the data title check is NO.

Figure 15 is a detailed flow chart of the process "D" shown in Fig. 11B. In the E WRITE 2 process, an E write finished check is carried out. Namely, it is determined whether or not the preceding E write 1 proc-

ess was completed without error. If the result is YES, the resultant information is checked. The resultant information indicates, for example, whether or not an overwrite has occurred in the external memory (EMEM). If the result of the check is NO, the error response is edited. If the check of the resultant information indicates a normal result, then a normal completion of the write process is recorded (memo). If the check indicates an abnormal result, then an abnormal completion of the write process is recorded (memo). The normal response is then edited, wherein the term "normal" means that the flow per se was completed normally and is not concerned with the above mentioned abnormal completion of the write process.

Figure 16 is a detailed flow chart of the process "E" shown in Fig. 11B. In the E READ 1 process, the open finish check is carried out as in the flow chart of Fig. 14. If the result of the check is YES, a data title check is started, as in the flow chart of Fig. 14. If the result of the check is YES, the corresponding address is found by the address holding means (shown by 44 in Fig. 7), as in the flow chart of Fig. 14, and then edited. The remaining steps are similar to those explained before.

Figure 17 is a detailed flow chart of the process "F" shown in Fig. 11B. In the E READ 2 process, the E read 1 finished check is carried out in the same as the corresponding step in Fig. 15. If the result is YES, the corresponding cipher key is found, and using the key, the read data is deciphered to edit the read data. The remaining steps are similar to those explained before.

Figure 18 is a detailed flow chart of the process "G" shown in Fig. 11B. In the E DELETE process, an open finished check is carried out, and if the result of the check is YES, a data title check is carried out. If the result of this check is YES, the corresponding address is found and edited to delete the content of the directory (shown by 21 in Fig. 5). The remaining steps are similar to those explained before.

Figure 9 is a detailed flow chart of the process "H" shown in Fig. 11B. In the VERIFY PIN process, an authentication check for an input PIN data is carried out. The remaining steps are similar to those explained before.

Figure 20 is a detailed flow chart of the process "I" shown in Figure 11B. In the CREATE E FILE process, a validity check for the system information directory is carried out, and if the result of the check is YES, then a validity of the CREATE is checked. If the result of this check is YES, a file registration is carried out. The remaining steps are the same as described previously. The validity of the CREATE is checked to confirm whether the file is created as required. If the result of the validity check is YES, the registration of the file to be created is carried out. The remaining steps are similar to those explained before.

Figure 21 is a detailed flow chart of the process "J" shown in Fig. 11B. In the CREATE E DIR process, the directory for the newly introduced file is created. First, double registration is checked to avoid a registration conflict. If the result of the check is YES, then it is determined whether or not a sufficient directory area exists. If the result of the check is YES, a registration to the directory is carried out. The remaining steps are similar to those explained before.

As understood from the above description, the IC card 10 is provided, as one body, with the external memory (EMEM) 11, which has a very large memory capacity, and therefore it is possible to store a vast amount of information, for example, video information. Specifically, it is possible to record, for example, a photograph of the user's face, the user's voice, the user's signature, the user's fingerprints, and so on. Of course, it is also possible to store information which overflows from the internal memory (IMEM) 5. The date may also be recorded simultaneously, since information such as for example, a photograph of the user's face, will not represent the user's face after a period of time. The date of the record is also important for, for example, a driving licence, a passport, and the like.

According to an embodiment of the present invention, a memory history management area can be created. The memory history management area manages information, such as mentioned above, to be stored in the external memory (EMEM) 11.

Figure 22 is a schematic diagram of the general construction of devices mounted in and on an IC card, in particular a memory history management part according to an embodiment of the invention. The arrangement of Fig. 22 is a modification of the arrangement shown in Fig. 5, explained previously. The history management part 70 is composed of at least a memory history directory 71 formed in the first directory 21 (Fig. 5). The memory history directory 71 preferably cooperates with a history record area 72 formed in the internal memory (IMEM), i.e. the file 9 (Fig. 5). The history directory 71 and the record area 72 are controlled by the processor (CPU) 4, in particular by the external memory access means (EMAM) 23.

Figures 23A and 23B show a specific arrangement of a memory history management part shown in Fig. 22. The data files in the external memory may be used with a regulated format as shown by 11 in Fig. 23B or a free format as shown by 11'. The external memory (EMEM) 11 (left side in Fig. 23B) is formatted as a plurality of blocks, such as B_1, B_2 --- B_n. In the example, block B_1 is allotted to photograph data, B_2 to voice data, B_3 to fingerprint data, B_4 to signature data, and B_5 to overflow data from the internal memory (IMEM) 5. Each of the blocks B_1 through B_n is composed of a plurality of sections S_1 through S_m.

As shown in Fig. 23A, the internal memory (IMEM) 5 contains therein the memory history direc-

tory 71 and the history record area 72, as the memory history management part 70 (Fig. 22). The memory history directory 71 indicates physical addresses on the external memory (EMEM) 11. The history record area 72 is divided with a plurality of rows, and each row is predefined by both block numbers B_1, B_2 --- B_n and section numbers S_1, S_2 --- S_m. Therefore, each time a write operation to the blocks B_1 thorugh B_n of Fig.23B is carried out, the date on which the related write operation was made is recorded in the corresponding row of the history record area 72 (Fig. 23A).

Figures 24A and 24B are a flow chart of the read and write operations to an external memory (EMEM), and also depict an arrangement of the related memories. The content of Fig. 24A is substantially the same as the content shown in Figs. 23A and 23B. The processing flow of Fig. 24B is programmed in the external memory access means (EMAM) 23 in Fig. 23A and the program is executed by the external IC card acceptance means 20 (terminal machine) and, if necessary, the terminal station 30. The communication is handled by the reader-writer and the reading and writing device.

When a read command and the corresponding logical address are sent from the acceptance means 20, a read operation is started by the processor (CPU) 4 in the IC card 10 (refer to "a" in Fig. 24B). This command is a request to scan the history, and thus a corresponding search in the history directory 71 is carried out ("b") and the physical address corresponding to the searched logical address is found. Using the found physical address, data is read from the EMEM 11 by the acceptance means 20 ("c"), and thereafter, the date on which the related read operation was carried out is written in the history directory 71 by the CPU 4 ("d"). The thus read data is sent to a demander of the related read request, e.g. the terminal station 30, by the acceptance means 20 ("e").

When a write command, the corresponding logical address, and the corresponding write data are received by the CPU 4 ("f"), the CPU 4 (Fig. 23A) carries out a search of the history directory 71 using the given logical address, to find the corresponding physical address ("g"). Based on the found physical address, the related write operation is carried out by the acceptance means 20 ("h"), and thereafter, the date on which the write operation was carried out is recorded by the CPU 4 ("i"). The result of the write operation is sent to the demander of the related write request, e.g., the terminal station 30, by the acceptance means 20 ("j").

As explained above in detail, an IC card of a system embodying the invention can handle a vast amount of data compared to the conventional IC card 1. Although the external memory (EMEM) is exposed outside the body of the IC card, security for the data stored therein can be assured because the EMEM is governed by the internal CPU alone.

Claims

1. An IC card (10) containing a processor (4), for communicating with an external card-acceptance device (20), and an internal memory (5), connected to cooperate with the processor (4), for storing data to be accessed by the processor (4), there being mounted on a surface of the card (10) an external memory (11) for storing further data, which further data is to be accessible only by way of the said external card-acceptance device (20),

   characterised in that the said internal memory (5) includes a directory (21,44) for storing respective addresses at which data files (19) are stored in the external memory (11), and in that the said processor (4) is provided with an external memory access program for enabling such a card-acceptance device (20) to obtain, from the said directory (21), address information necessary to enable the card-acceptance device (20) to access such files in the external memory (11).

2. An IC card as claimed in claim 1, wherein the said external memory (11) has a memory capacity larger than that of the said internal memory (5).

3. An IC card as claimed in claim 1 or 2, wherein the said external memory (11) is an optical memory.

4. An IC card as claimed in claim 3, wherein the said external memory (11) is a laser memory.

5. An IC card as claimed in any preceding claim, wherein data can only be stored in the said external memory (11) under control of the said processor (4).

6. An IC card as claimed in any one of claims 1 to 4, wherein the read and write operations for the said external memory (11) are carried out by using only addresses handled by the said processor (4).

7. An IC card as set forth in any preceding claim, wherein user identity data relating to an IC card owner is stored in the said external memory (11).

8. An IC card as claimed in any preceding claim, wherein the said external memory (11) contains a password area (17) used for an authentication check of said external memory (11) by the said processor (4).

9. An IC card as claimed in claim 7, wherein an address at which new data is to be written in the external memory (11) is selected from the said directory (21) by finding therein an external mem-

ory address denoted in that directory as being vacant.

10. An IC card as claimed in any preceding claim, wherein cryptographic management information is stored in the said internal memory (5), for use in enciphering and deciphering data passed between the said processor (4) and the said external memory (11) by way of the said card-acceptance device (20).

11. An IC card as claimed in claim 10, wherein the said processor includes a write processing means (43), a first read processing means (41) and a second read processing means (42),

the said write processing means (43) being operable, upon receipt of a write command and the corresponding write data, to encipher the received write data with reference to the said cryptographic management information, to search the said directory (21) for an address, in the said external memory (11), at which the enciphered write data is to be written, and to send the enciphered write data and the corresponding address to the card-acceptance device (20),

the said first read processing means (41) being operable, upon receipt of a first read command and an individual file number of a required data file in the external memory (11), to search the said directory (21) for the read address corresponding to the said individual file number and to send that address to the card-acceptance device (20), and

the said second read processing means (42) being operable, upon receipt of a second read command and enciphered read data, to decipher the received enciphered read data, with reference to the said cryptographic management information, and to send the deciphered read data to the card-acceptance device (20).

12. An IC card as claimed in claim 10, wherein the said external card-acceptance device (20) cooperates, when the said processor (4) is to perform a write operation, with the said IC card, so that the write command and corresponding write data are sent to the IC card, enciphered write data and the corresponding address for writing in the external memory (11) are obtained from the IC card, and the enciphered write data is written in the external memory (11).

13. An IC card as claimed in claim 10 or 12, wherein the said external card-acceptance device (20) cooperates, when the said processor (4) is to perform a read operation, with the IC card, so that a first read command and an individual file number are sent to the IC card, the required read address corresponding to the individual file number is obtained from the IC card by searching the said directory (21) and that read address is sent to the card-acceptance device (20), enciphered read data is obtained from the external memory (11) by using the said read address, the enciphered read data from the external memory (11) is sent to the IC card with a second read command, and deciphered read data is sent from the IC card to the said card-acceptance device (20) in response to the second read command.

14. An IC card as claimed in any preceding claim, wherein the internal memeory (5) includes memory history management means, for managing historical information relating to the storage of data in the said external memory (11).

15. An IC card as claimed in claim 14, wherein the said directory (21)includes a memory history directory (71).

16. An IC card as claimed in claim 15, wherein the said internal memory (5) includes a history record area (72), management of the said historical information being performed by the said processor (4) in cooperation with the said history record area (72) and the said memory history directory (71).

17. An IC card as claimed in claim 16, wherein the said history record area (72) serves to store a date on which a read or write operation was carried out from or to the said external memory (11).

18. An IC card as claimed in claim 16 or 17, wherein the said memory history directory (71) serves to correlate data entries in the said history record area (72) with the respective corresponding addresses in the said external memory (11).

19. An IC card as claimed in claim 18, wherein data stored at the said respective corresponding addresses represents a photograph of a face, and/or a voice, and/or a fingerprint, and/or a signature of an IC card user.

20. An IC card as claimed in claim 18 or 19, wherein data stored at the said respective corresponding addresses comprises data which overflows from the said internal memory (5) owing to a lack of sufficient memory capacity thereof.

21. An IC card as claimed in any preceding claim, wherein the said internal memory (5) is a non-volatile memory.

22. An IC card as claimed in any preceding claim,

wherein the said internal memory (5) is an electronically erasable programmable read only memory (EEPROM).

23. An IC card as claimed in any preceding claim, in combination with an external card-acceptance device (20) operative on the basis of address data read by the device from the said internal memory (5) to access data in the said external memory (11).

Patentansprüche

1. IC-Karte (10), welche einen Prozessor (4) zum Kommunizieren mit einer externen Kartenannahmeanordnung (20) und einen internen Speicher (5), der angeschlossen ist, um mit dem Prozessor (4) zusammenzuarbeiten, zum Speichern von Daten, die für den Prozessor (4) zugängig sind, enthält, wobei auf einer Fläche der Karte (10) ein externer Speicher (11) zum Speichern weiterer Daten montiert ist, welche weiteren Daten nur mittels der genannten externen Kartenannahmeanordnung (20) zugängig sind,

dadurch gekennzeichnet, daß der genannte interne Speicher (5) ein Verzeichnis (21, 44) zum Speichern entsprechender Adressen, an denen Datendateien (15) im externen Speicher gespeichert sind, enthält, und daß der genannte Prozessor (4) mit einem externen Speicherzugriffsprogramm versehen ist, um zu ermöglichen, daß eine derartige Kartenannahmeanordnung (20), vom genannten Verzeichnis (21), Adresseninformationen erhält, die notwendig sind, um zu ermöglichen, daß die Kartenannahmeanordnung (20) auf derartige Dateien im externen Speicher (11) zugreift.

2. IC-Karte nach Anspruch 1, bei welcher der genannte externe Speicher (11) eine größere Speicherkapazität als jene des genannten internen Speichers (5) aufweist.

3. IC-Karte nach Anspruch 1 oder 2, bei welcher der genannte externe Speicher (11) ein optischer Speicher ist.

4. IC-Karte nach Anspruch 3, bei welcher der genannte externe Speicher (11) ein Laserspeicher ist.

5. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher Daten nur im genannten Speicher (11) unter der Steuerung des genannten Prozessors (4) gespeichert werden können.

6. IC-Karte nach einem der Ansprüche 1 bis 4, bei welcher die Schreib- und Leseoperationen für den genannten externen Speicher (11) nur unter Verwendung von vom genannten Prozessor (4) bearbeiteten Adressen durchgeführt werden.

7. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher Benutzeridentitätsdaten in bezug auf einen IC-Kartenbesitzer im genannten externen Speicher (11) gespeichert werden.

8. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher der genannte externe Speicher (11) einen Paßwortbereich (17), der zur Authentisierungsprüfung des genannten externen Speichers (11) durch den genannten Prozessor (4) verwendet wird, enthält.

9. IC-Karte nach Anspruch 7, bei welcher eine Adresse, an der neue Daten in den externen Speicher (11) zu schreiben sind, aus dem genannten Verzeichnis (21) ausgewählt wird, indem darin eine externe Speicheradresse, die in diesem Verzeichnis als frei bezeichnet ist, aufgefunden wird.

10. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher kryptographische Verwaltungsinformationen im genannten internen Speicher (5) zur Verwendung bei der Verschlüsselung und Entschlüsselung von Daten, die zwischen dem genannten Prozessor (4) und dem genannten externen Speicher (11) mittels der genannten Kartenannahmeanordnung (20) weitergereicht werden, gespeichert werden.

11. IC-Karte nach Anspruch 10, bei welcher der genannte Prozessor eine Schreibverarbeitungseinrichtung (43), eine erste Leseverarbeitungseinrichtung (41) und eine zweite Leseverarbeitungseinrichtung (42) enthält,

wobei die genannte Schreibverarbeitungseinrichtung (43), beim Empfang eines Schreibbefehls und der entsprechenden Schreibdaten, betreibbar ist, um die empfangenen Schreibdaten unter Bezugnahme auf die genannten kryptographischen Verwaltungsinformationen zu verschlüsseln, das genannte Verzeichnis (21) nach einer Adresse im genannten externen Speicher (11) zu durchsuchen, an der die verschlüsselten Schreibdaten zu schreiben sind, und die verschlüsselten Schreibdaten und die entsprechende Adresse an die Kartenannahmeanordnung (20) zu senden,

wobei die genannte erste Leseverarbeitungseinrichtung (41), beim Empfang eines ersten Lesebefehls und einer einzelnen Dateinummer einer erforderlichen Datei im externen Speicher (11), betreibbar ist, um das genannte Ver-

zeichnis (21) nach der Leseadresse, die der genannten einzelnen Dateinummer entspricht, zu durchsuchen, und diese Adresse an die Kartenannahmeanordnung (20) zu senden, und

wobei die genannte zweite Leseverarbeitungseinrichtung (42), beim Empfang eines zweiten Lesebefehls und von verschlüsselten Lesedaten, betreibbar ist, um die empfangenen verschlüsselten Lesedaten unter Bezugnahme auf die genannten kryptographischen Verwaltungsinformationen zu entschlüsseln, und die entschlüsselten Lesedaten an die Kartenannahmeanordnung (20) zu senden.

12. IC-Karte nach Anspruch 10, bei welcher die genannte externe Kartenannahmeanordnung (20), wenn der genannte Prozessor (4) eine Schreiboperation durchzuführen hat, mit der genannten IC-Karte zusammenarbeitet, so daß der Schreibbefehl und entsprechende Schreibdaten an die IC-Karte gesendet werden, verschlüsselte Schreibdaten und die entsprechende Adresse zum Schreiben im externen Speicher (11) von der IC-Karte erhalten werden, und die verschlüsselten Schreibdaten in den externen Speicher (11) geschrieben werden.

13. IC-Karte nach Anspruch 10 oder 12, bei welcher die genannte externe Kartenannahmeanordnung (20), wenn der genannte Prozessor (4) eine Leseoperation durchzuführen hat, mit der genannten IC-Karte zusammenarbeitet, so daß ein erster Lesebefehl und eine einzelne Dateinummer an die IC-Karte gesendet werden, die erforderliche Leseadresse, die der einzelnen Dateinummer entspricht, von der IC-Karte erhalten wird, indem das genannte Verzeichnis (21) durchsucht wird, und diese Leseadresse an die Kartenannahmeanordnung (20) gesendet wird, verschlüsselte Lesedaten vom externen Speicher (11) unter Verwendung der genannten Leseadresse erhalten werden, die verschlüsselten Lesedaten vom externen Speicher (11) zur IC-Karte mit einem zweiten Lesebefehl gesendet werden, und entschlüsselte Lesedaten von der IC-Karte zur genannten Kartenannahmeanordnung (20) ansprechend auf den zweiten Lesebefehl gesendet werden.

14. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher der interne Speicher (5) eine Speicherprotokoll-Verwaltungseinrichtung zum Verwalten von Protokollinformationen in bezug auf die Speicherung von Daten im genannten externen Speicher (11) enthält.

15. IC-Karte nach Anspruch 14, bei welcher das genannte Verzeichnis (21) ein Speicherprotokollverzeichnis (71) enthält.

16. IC-Karte nach Anspruch 15, bei welcher der genannte interne Speicher (5) einen Protokolldatensatzbereich (72) enthält, wobei die Verwaltung der genannten Protokollinformationen vom genannten Prozessor (4) in Zusammenarbeit mit dem genannten Protokolldatensatzbereich (72) und dem genannten Speicherprotokollverzeichnis (71) durchgeführt wird.

17. IC-Karte nach Anspruch 16, bei welcher der genannte Protokolldatensatzbereich (72) dazu dient, ein Datum, zu dem eine Lese- oder Schreiboperation aus oder in dem genannten externen Speicher (11) durchgeführt wurde, zu speichern.

18. IC-Karte nach Anspruch 16 oder 17, bei welcher das genannte Speicherprotokollverzeichnis (71) dazu dient, Dateneinträge im genannten Protokolldatensatzbereich (72) mit den jeweiligen entsprechenden Adressen im genannten externen Speicher (11) zu korrelieren.

19. IC-Karte nach Anspruch 18, bei welcher Daten, die an den genannten jeweiligen entsprechenden Adressen gespeichert werden, eine Photographie eines Gesichts und/oder eine Stimme und/oder einen Fingerabdruck und/oder eine Unterschrift eines IC-Kartenbenutzers repräsentieren.

20. IC-Karte nach Anspruch 18 oder 19, bei welcher Daten, die an den genannten jeweiligen entsprechenden Adressen gespeichert werden, Daten umfassen, die vom genannten internen Speicher (5) auf Grund eines Mangels an ausreichender Speicherkapazität davon überlaufen.

21. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher der genannte interne Speicher (5) ein nicht-flüchtiger Speicher ist.

22. IC-Karte nach einem der vorhergehenden Ansprüche, bei welcher der genannte interne Speicher (5) ein elektronisch löschbarer, programmierbarer Festwertspeicher (EEPROM) ist.

23. IC-Karte nach einem der vorhergehenden Ansprüche, in Kombination mit einer externen Kartenannahmeanordnung (20), betreibbar auf Basis von Adressendaten, die von der Anordnung aus dem genannten internen Speicher (5) gelesen werden, um auf Daten im genannten externen Speicher (11) zuzugreifen.

Revendications

1. Carte à circuit intégré (IC) (10) contenant un processeur (4) pour communiquer avec un dispositif d'acceptation de carte externe (20), et une mémoire interne (5), connectée pour coopérer avec le processeur (4), pour stocker des données destinées à être accédées par le processeur (4), une mémoire externe (11), permettant de stocker des données supplémentaires, lesquelles données supplémentaires sont destinées à être accédées seulement au moyen dudit dispositif d'acceptation de carte externe (20), étant montée sur la surface de la carte (10),

   caractérisé en ce que ladite mémoire interne (5) inclut un répertoire (21, 44) pour stocker des adresses respectives au niveau desquelles des fichiers (19) sont stockés dans la mémoire externe (11), et en ce que ledit processeur (4) est muni d'un programme d'accès de mémoire externe pour permettre à ce dispositif d'acceptation de carte (20) d'obtenir, à partir dudit répertoire (21), une information d'adresse nécessaire pour permettre au dispositif d'acceptation de carte (20) d'accéder au fichier contenu dans la mémoire externe (11).

2. Carte à IC selon la revendication 1, dans laquelle ladite mémoire externe (11) présente une capacité mémoire supérieure à celle de ladite mémoire interne (5).

3. Carte à IC selon la revendication 1 ou 2, dans laquelle ladite mémoire externe (11) est une mémoire optique.

4. Carte à IC selon la revendication 3, dans laquelle ladite mémoire externe (11) est une mémoire laser.

5. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle des données peuvent seulement être stockées dans ladite mémoire externe (11) sous la commande dudit processeur (4).

6. Carte à IC selon l'une quelconque des revendications 1 à 4, dans laquelle les opérations de lecture et d'écriture pour ladite mémoire externe (11) sont mises en oeuvre en utilisant seulement des adresses manipulées par ledit processeur (4).

7. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle des données d'identification d'utilisateur concernant un détenteur de carte à IC sont stockées dans ladite mémoire externe (11).

8. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle ladite mémoire externe (11) contient une zone de mot de passe (17) utilisée pour un contrôle d'authentification de ladite mémoire externe (11) par ledit processeur (4).

9. Carte à IC selon la revendication 7, dans laquelle une adresse au niveau de laquelle de nouvelles données doivent être écrites dans la mémoire externe (11) est choisie dans ledit répertoire (20) en recherchant en son sein une adresse de mémoire externe indiquée dans ce répertoire comme étant vacante.

10. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle une information de gestion cryptographique est stockée dans ladite mémoire interne (5) en vue d'une utilisation pour chiffrer et déchiffrer des données passées entre ledit processeur (4) et ladite mémoire externe (11) au moyen dudit dispositif d'acceptation de carte (20).

11. Carte à IC selon la revendication 7, dans laquelle ledit processeur inclut un moyen de traitement d'écriture (43), un premier moyen de traitement de lecture (41) et un second moyen de traitement de lecture (42),

    ledit moyen de traitement d'écriture (43) pouvant fonctionner, suite à la réception d'une commande d'écriture et des données d'écriture correspondantes, pour chiffrer les données d'écriture reçues par référence à ladite information de gestion cryptographique afin de rechercher une adresse dans ledit répertoire (21), dans ladite mémoire externe (11), adresse au niveau de laquelle les données d'écriture chiffrées doivent être écrites, et afin d'envoyer les données d'écriture chiffrées et l'adresse correspondante au dispositif d'acceptation de carte (20),

    ledit premier moyen de traitement de lecture (41) pouvant fonctionner suite à la réception d'une première commande de lecture et d'un numéro de fichier individuel d'un fichier de données requis contenu dans la mémoire externe (11) pour rechercher dans ledit répertoire (21) l'adresse de lecture correspondant audit numéro de fichier individuel et pour envoyer cette adresse au dispositif d'acceptation de carte (20) ; et

    ledit second moyen de traitement de lecture (42) pouvant fonctionner suite à la réception d'une seconde commande de lecture et de données de lecture chiffrées pour déchiffrer les données de lecture chiffrées reçues par référence à ladite information de gestion cryptographique et pour envoyer les données de lecture déchiffrées au dispositif d'acceptation de carte (20).

12. Carte à IC selon la revendication 10, dans laquelle ledit dispositif d'acceptation de carte externe (20) coopère, lorsque ledit processeur (4) doit réaliser une opération d'écriture, avec ladite carte à IC de telle sorte que la commande d'écriture et que des données d'écriture correspondantes soient envoyées à la carte IC, que des données d'écriture chiffrées et que l'adresse correspondante pour l'écriture dans la mémoire externe (11) soient obtenues à partir de la carte à IC et que les données d'écriture chiffrées soient écrites dans la mémoire externe (11).

13. Carte à IC selon la revendication 10 ou 12, dans laquelle ledit dispositif d'acceptation de carte externe (20) coopère, lorsque ledit processeur (4) doit réaliser une opération de lecture, avec la carte à IC de telle sorte qu'une première commande de lecture et qu'un numéro de fichier individuel soient envoyés à la carte à IC, que l'adresse de lecture requise correspondant au numéro de fichier individuel soit obtenue à partir de la carte à IC en recherchant ledit répertoire (21) et que l'adresse de lecture soit envoyée au dispositif d'acceptation de carte (20), que des données de lecture chiffrées soient obtenues depuis la mémoire externe (11) en utilisant ladite adresse de lecture, que les données lues chiffrées provenant de la mémoire externe (11) soient envoyées à la carte à IC à l'aide d'une seconde commande de lecture et que les données lues déchiffrées soient envoyées depuis la carte à IC audit dispositif d'acceptation de carte (20) en réponse à la seconde commande de lecture.

14. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle la mémoire interne (5) inclut un moyen de gestion d'historique de mémoire pour gérer une information d'historique concernant le stockage des données dans ladite mémoire externe (11).

15. Carte à IC selon la revendication 14, dans laquelle ledit répertoire (21) inclut un répertoire d'historique de mémoire (71).

16. Carte à IC selon la revendication 15, dans laquelle ladite mémoire interne (5) inclut une zone d'enregistrement d'historique (72), la gestion de ladite information d'historique étant réalisée par ledit processeur (4) en coopération avec ladite zone d'enregistrement d'historique (72) et avec ledit répertoire d'historique de mémoire (71).

17. Carte à IC selon la revendication 16, dans laquelle ladite zone d'enregistrement d'historique (72) sert à stocker une date à laquelle une opération de lecture ou d'écriture a été mise en oeuvre par rapport à ladite mémoire externe (11).

18. Carte à IC selon la revendication 16 ou 17, dans laquelle ledit répertoire d'historique de mémoire (71) sert à corréler des entrées de données dans ladite zone d'enregistrement d'historique (72) avec les adresses correspondantes respectives dans ladite mémoire externe (11).

19. Carte à IC selon la revendication 18, dans laquelle des données stockées au niveau desdites adresses correspondantes respectives représentent une photographie d'un visage et/ou une voix et/ou une empreinte digitale et/ou une signature d'un détenteur de carte à IC.

20. Carte à IC selon la revendication 18, dans laquelle des données stockées au niveau desdites adresses correspondantes respectives comprennent des données qui sont en dépassement par rapport à ladite mémoire interne (5) du fait du manque d'une capacité mémoire suffisante de celle-ci.

21. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle ladite mémoire interne (5) est une mémoire non volatile.

22. Carte à IC selon l'une quelconque des revendications précédentes, dans laquelle ladite mémoire interne (5) est une mémoire morte programmable et effaçable électroniquement (EEPROM).

23. Carte à IC selon l'une quelconque des revendications précédentes, en combinaison avec un dispositif d'acceptation de carte externe (20) qui fonctionne sur la base de données d'adresse lues par le dispositif dans ladite mémoire interne (5) afin d'accéder à des données contenues dans ladite mémoire externe (11).

Fig. 1

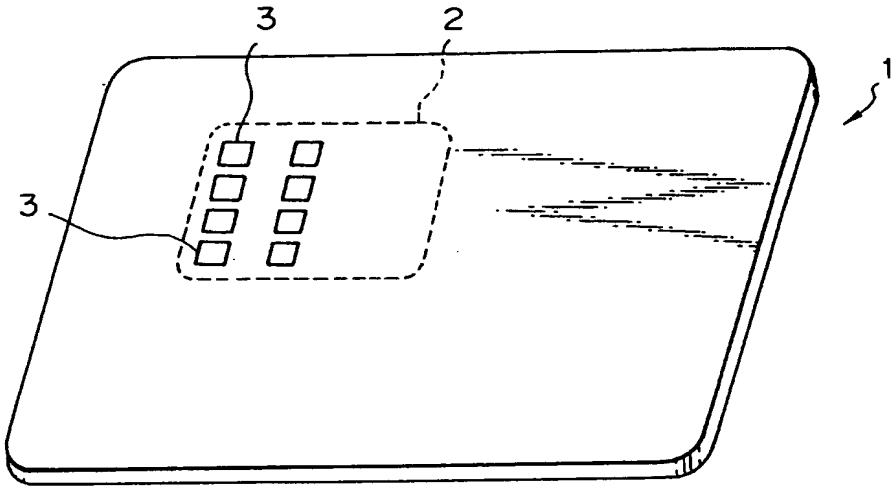

3
2
1
3

Fig. 2

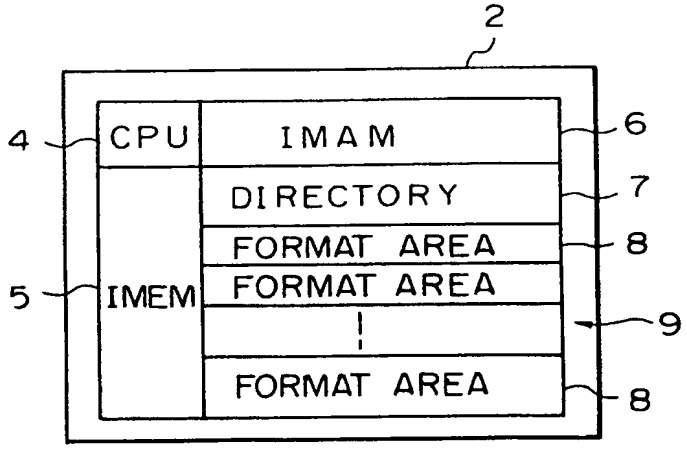

2
4
CPU
IMAM
6
DIRECTORY
7
FORMAT AREA
8
5
IMEM
FORMAT AREA
9
FORMAT AREA
8

Fig. 3

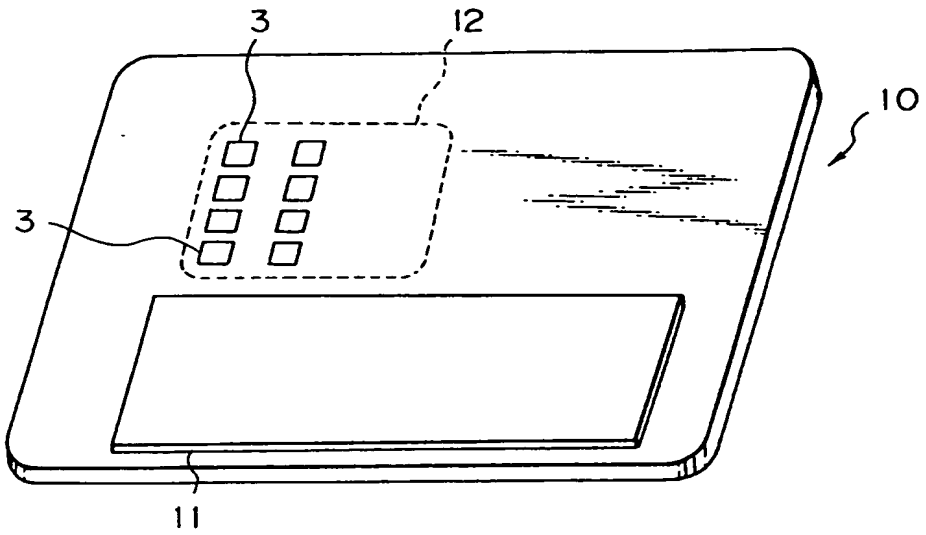


Fig. 4

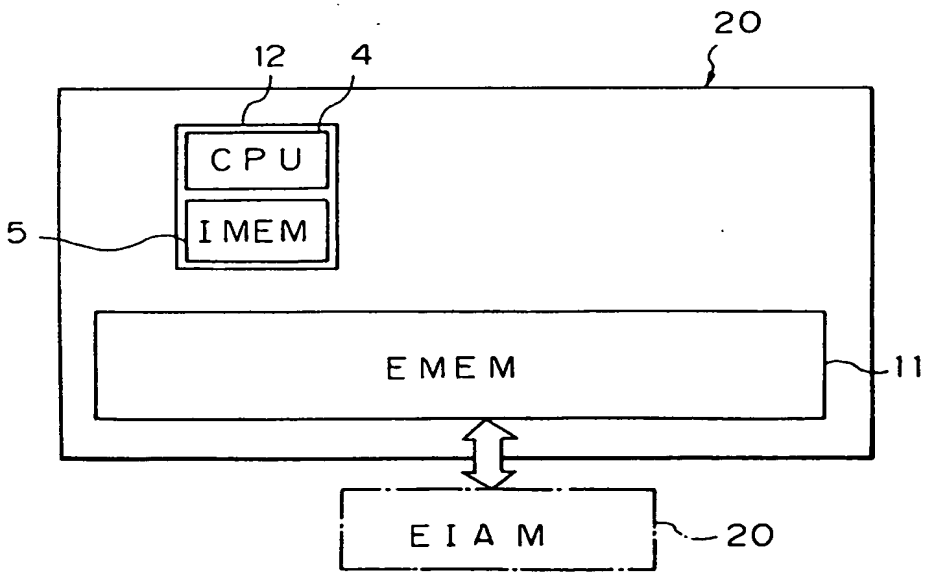


Fig. 5

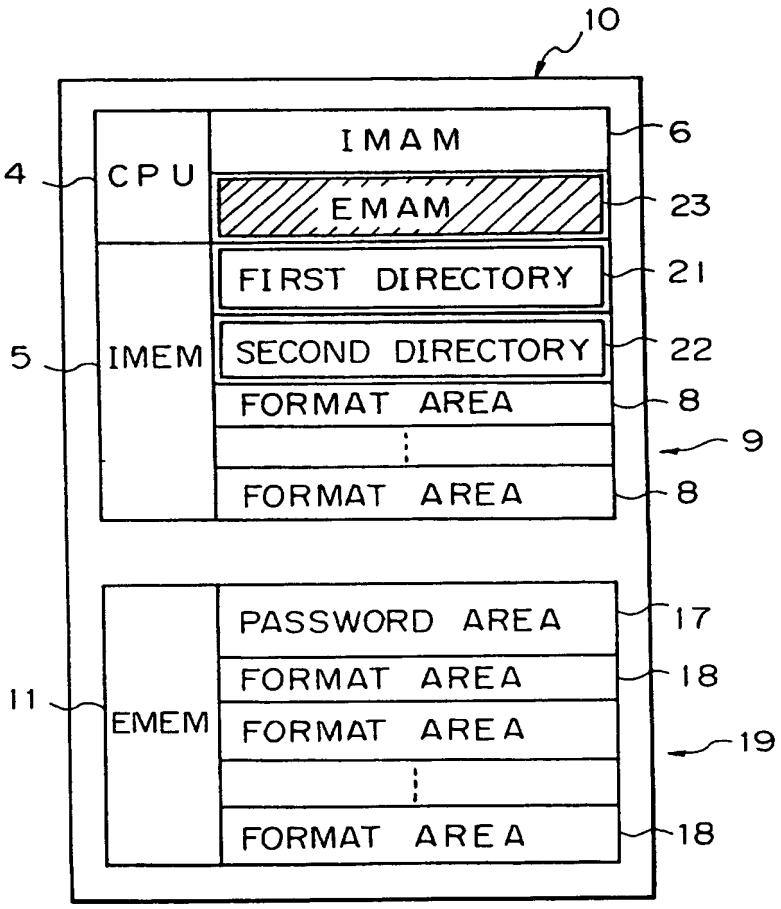

10
IMAM
6
4
CPU
EMAM
23
FIRST DIRECTORY
21
5
IMEM
SECOND DIRECTORY
22
FORMAT AREA
8
9
FORMAT AREA
8
PASSWORD AREA
17
FORMAT AREA
18
11
EMEM
FORMAT AREA
19
FORMAT AREA
18

Fig. 6

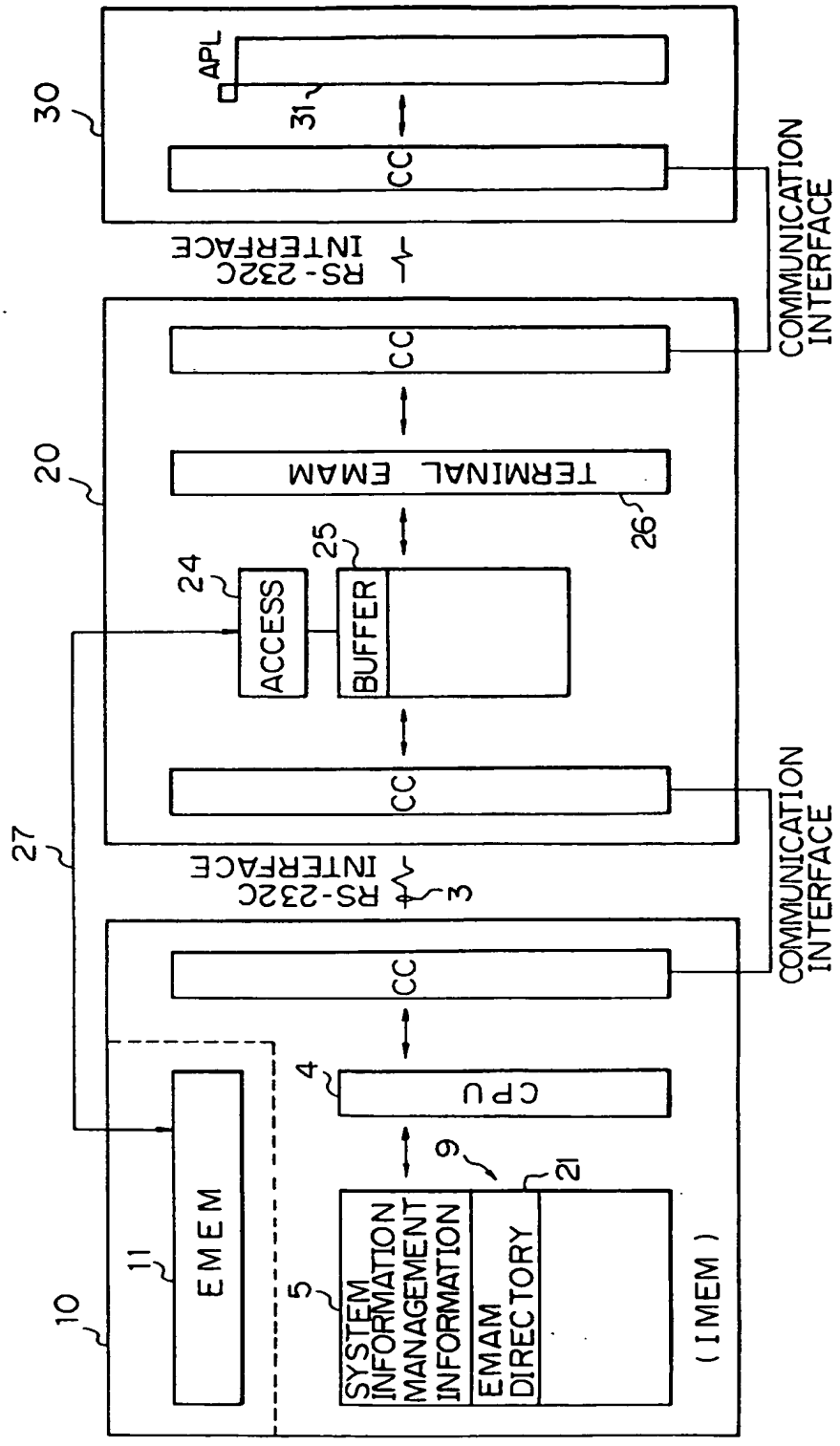

30
APL
31
CC
RS-232C INTERFACE
COMMUNICATION INTERFACE
20
CC
TERMINAL EMAM
26
24
ACCESS
25
BUFFER
CC
27
RS-232C INTERFACE
3
COMMUNICATION INTERFACE
CC
4
CPU
9
21
10
11
EMEM
5
SYSTEM INFORMATION
MANAGEMENT INFORMATION
EMAM DIRECTORY
(IMEM)

Fig. 7

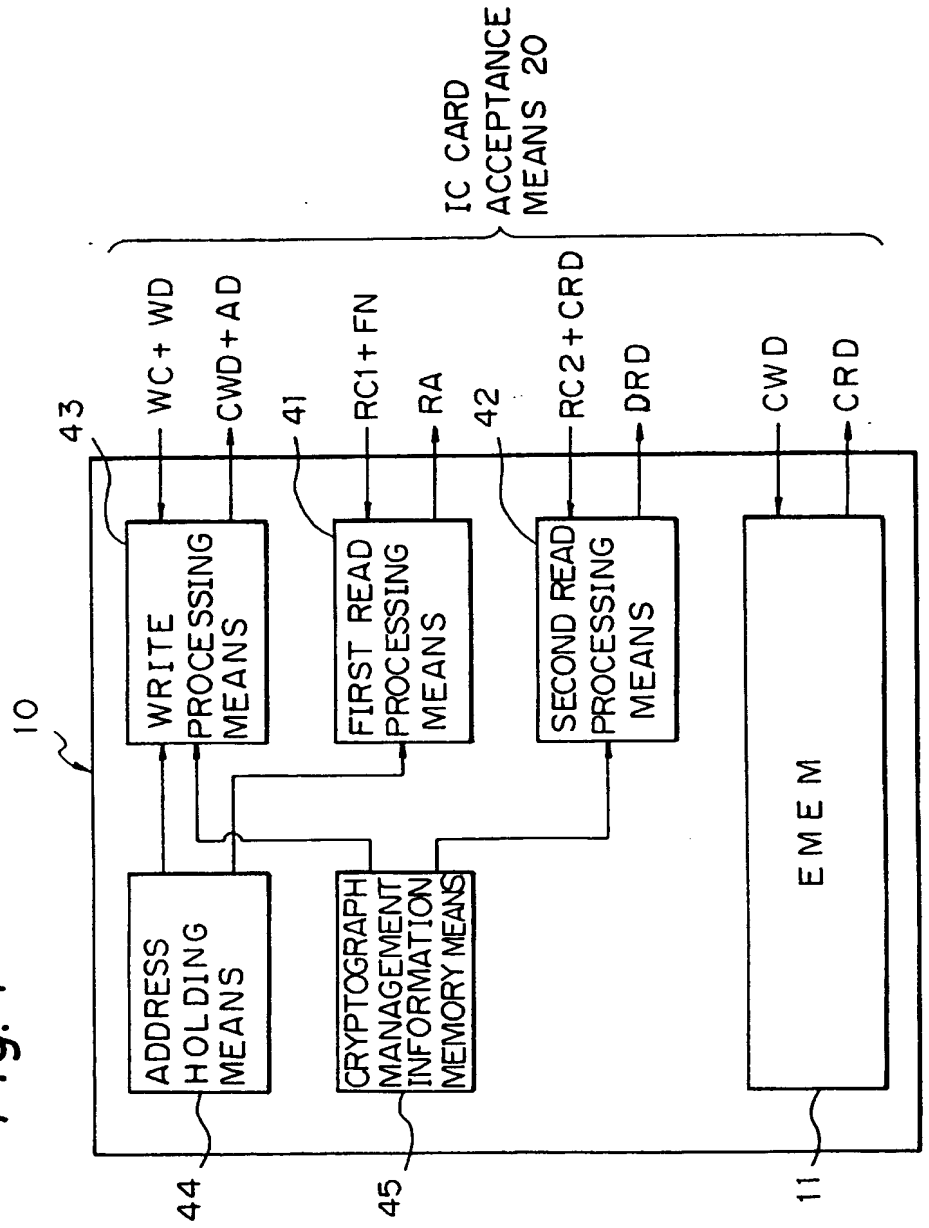
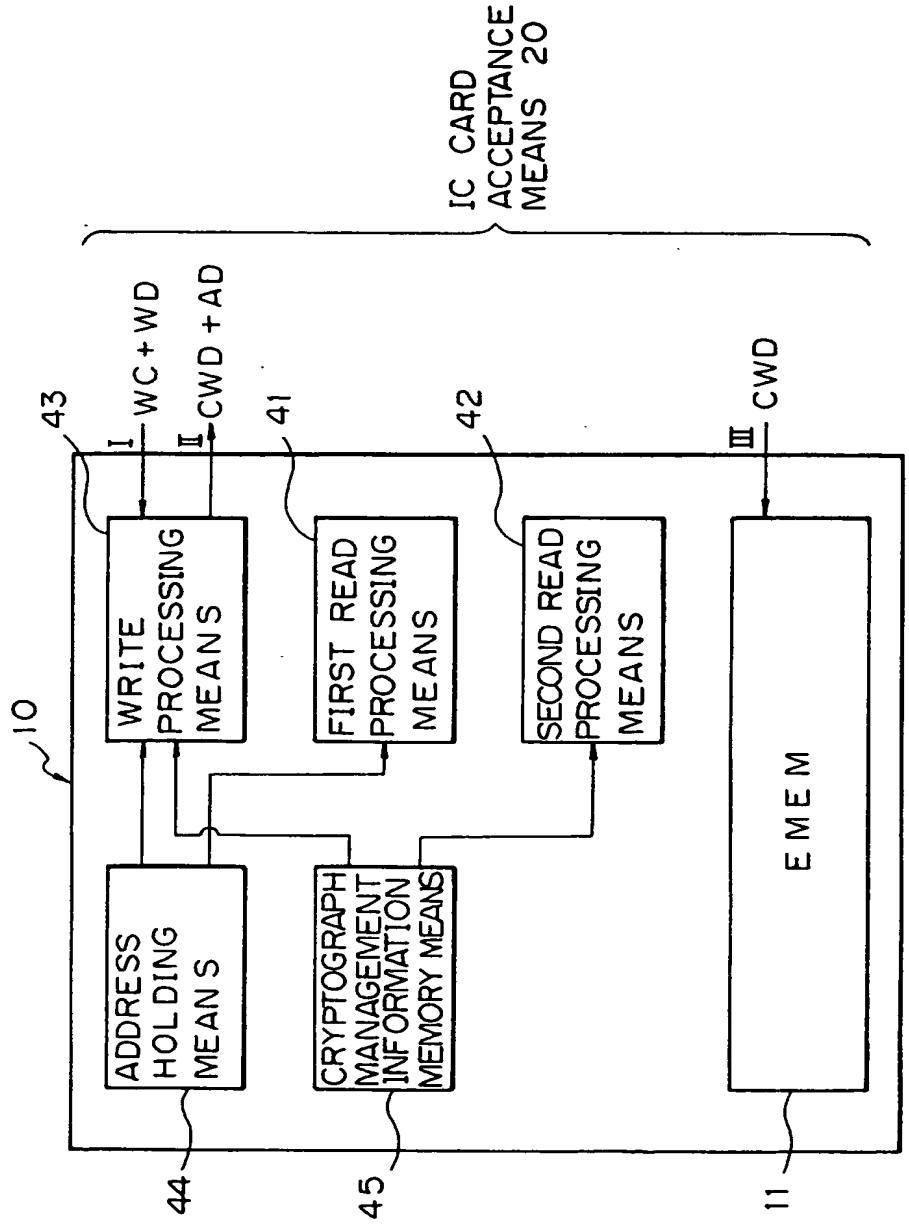

IC CARD ACCEPTANCE MEANS 20
WC + WD
CWD + AD
RC1 + FN
RA
RC2 + CRD
DRD
CWD
CRD
43
41
42
10
WRITE PROCESSING MEANS
FIRST READ PROCESSING MEANS
SECOND READ PROCESSING MEANS
EMEM
ADDRESS HOLDING MEANS
CRYPTOGRAPH MANAGEMENT INFORMATION MEMORY MEANS
44
45
11

Fig. 8


IC CARD ACCEPTANCE MEANS 20
WC + WD
CWD + AD
CWD
I
II
III
43
41
42
10
WRITE PROCESSING MEANS
FIRST READ PROCESSING MEANS
SECOND READ PROCESSING MEANS
EMEM
ADDRESS HOLDING MEANS
CRYPTOGRAPH MANAGEMENT INFORMATION MEMORY MEANS
44
45
11

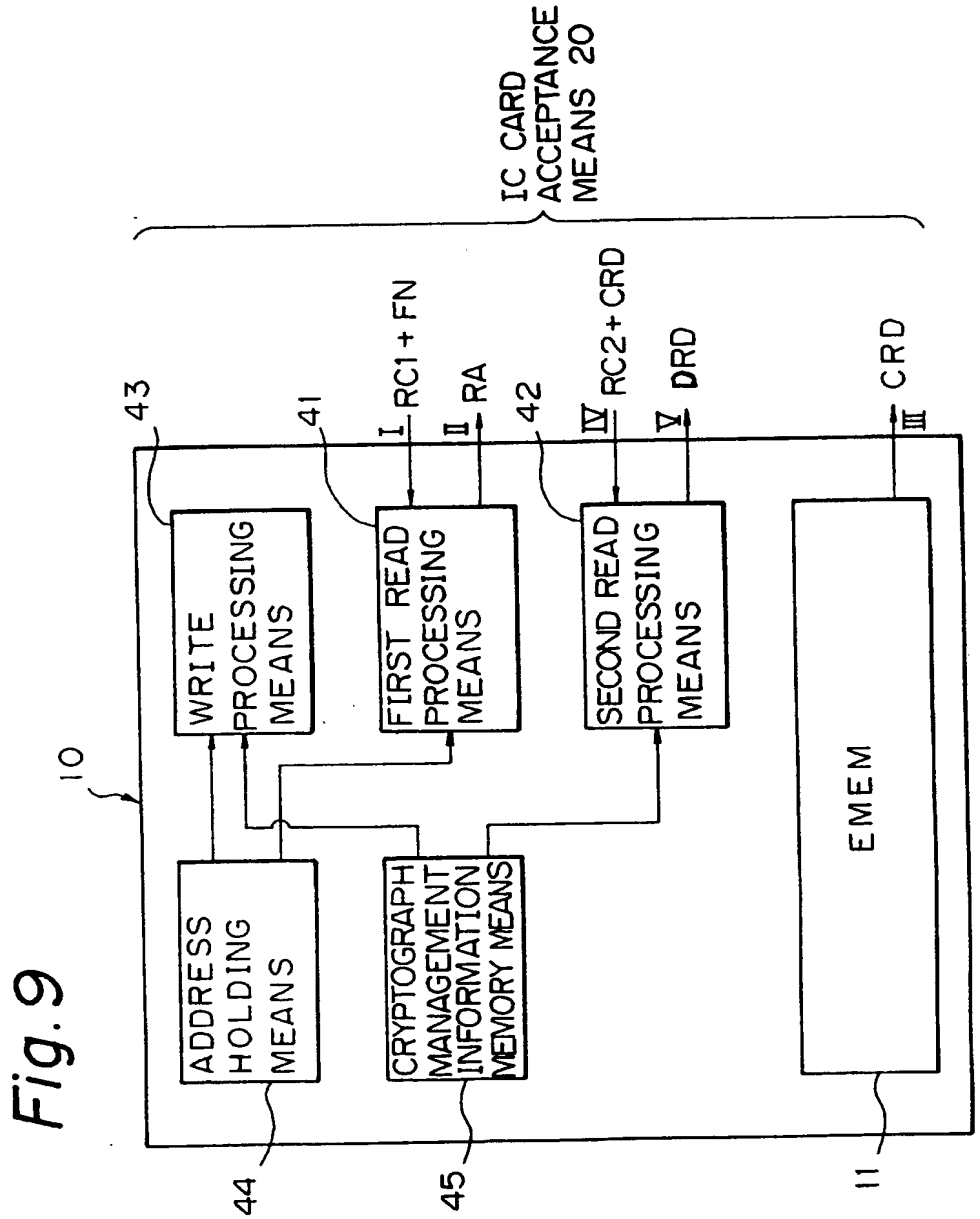

IC CARD ACCEPTANCE MEANS 20
10
43
41
42
I RC1 + FN
II RA
IV RC2 + CRD
V DRD
III CRD
WRITE PROCESSING MEANS
FIRST READ PROCESSING MEANS
SECOND READ PROCESSING MEANS
EMEM
ADDRESS HOLDING MEANS
CRYPTOGRAPH MANAGEMENT INFORMATION MEMORY MEANS
44
45
11

Fig. 9

Fig. 10

Fig. 10A | Fig. 10B

Fig. 10A

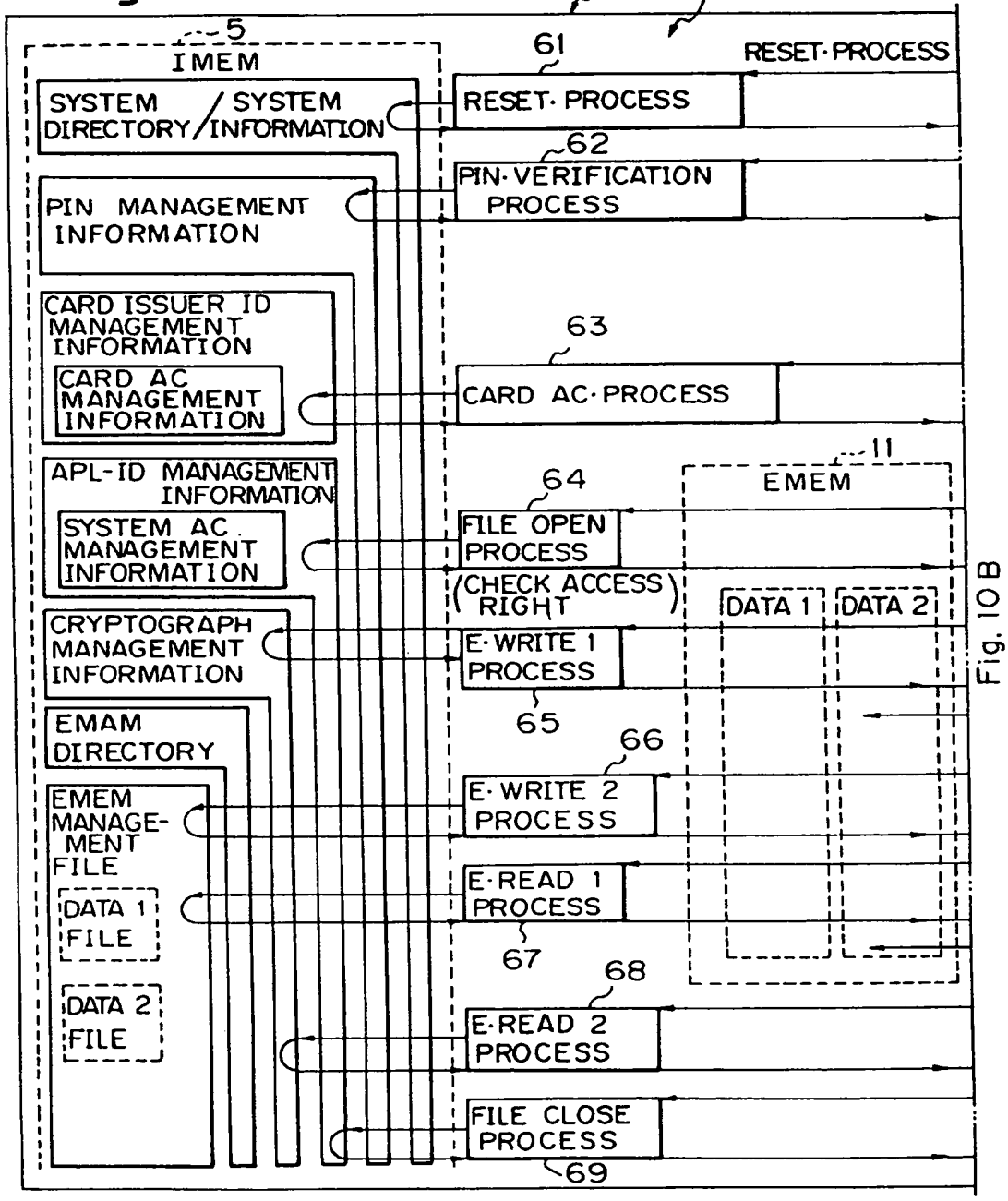


Fig. 10B

Fig. 10B

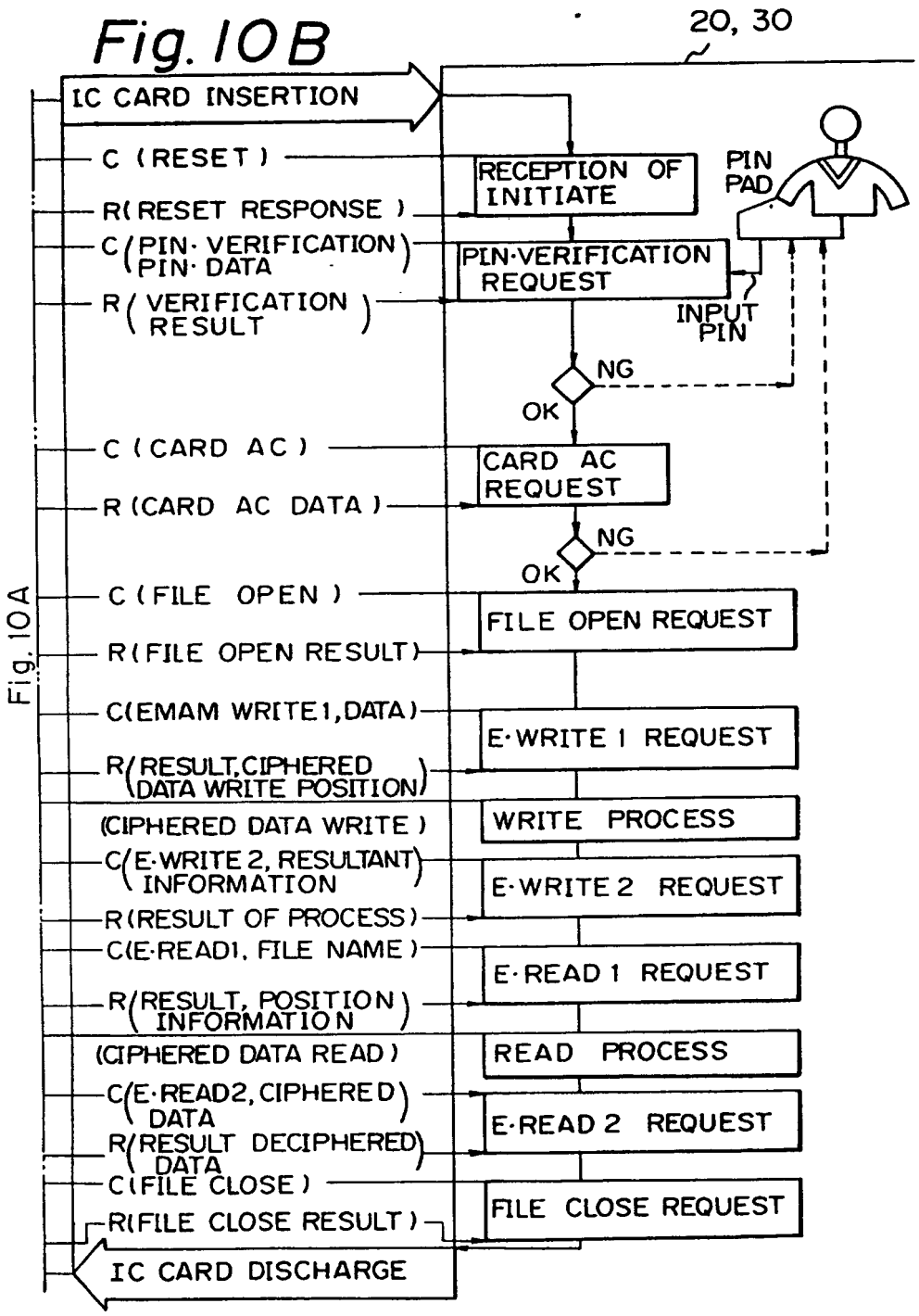


Fig. 10A

Fig.11

Fig.11A
Fig.11B

Fig. 11A

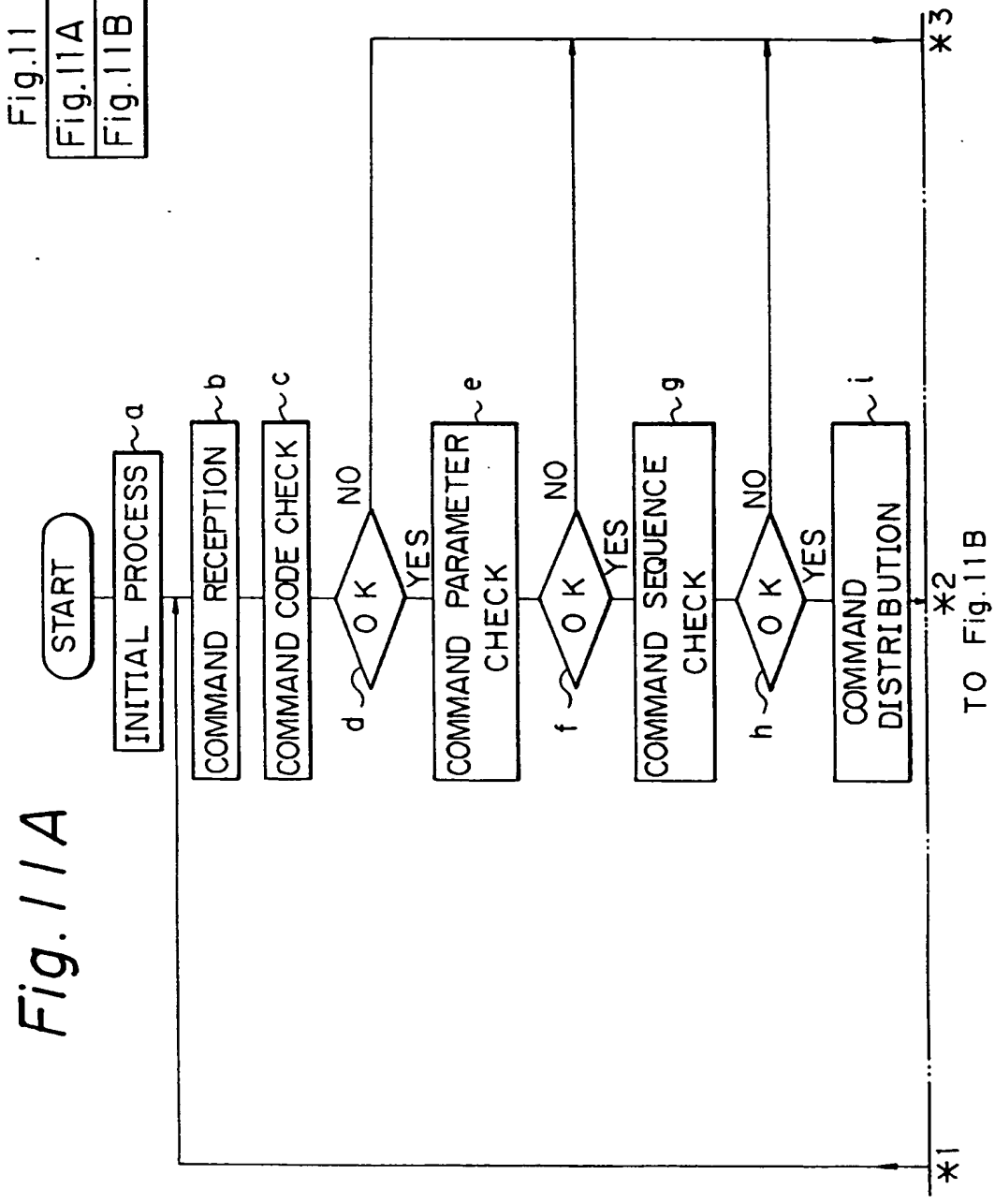


Fig. 11B

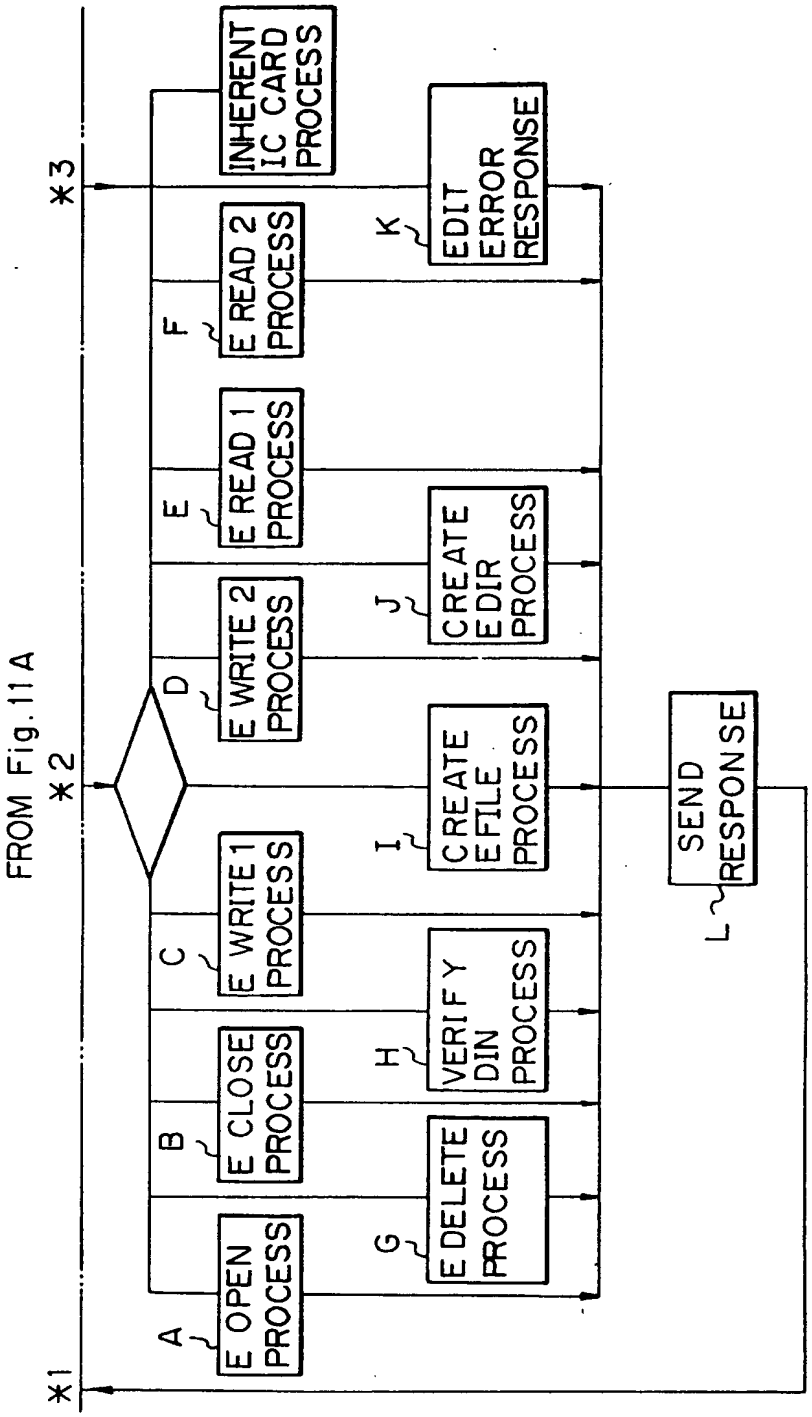

FROM Fig. 11A
*1
*2
*3
A
E OPEN PROCESS
B
E CLOSE PROCESS
C
E WRITE 1 PROCESS
D
E WRITE 2 PROCESS
E
E READ 1 PROCESS
F
E READ 2 PROCESS
G
E DELETE PROCESS
H
VERIFY DIN PROCESS
I
CREATE EFILE PROCESS
J
CREATE EDIR PROCESS
K
EDIT ERROR RESPONSE
INHERENT IC CARD PROCESS
L
SEND RESPONSE

Fig. 12

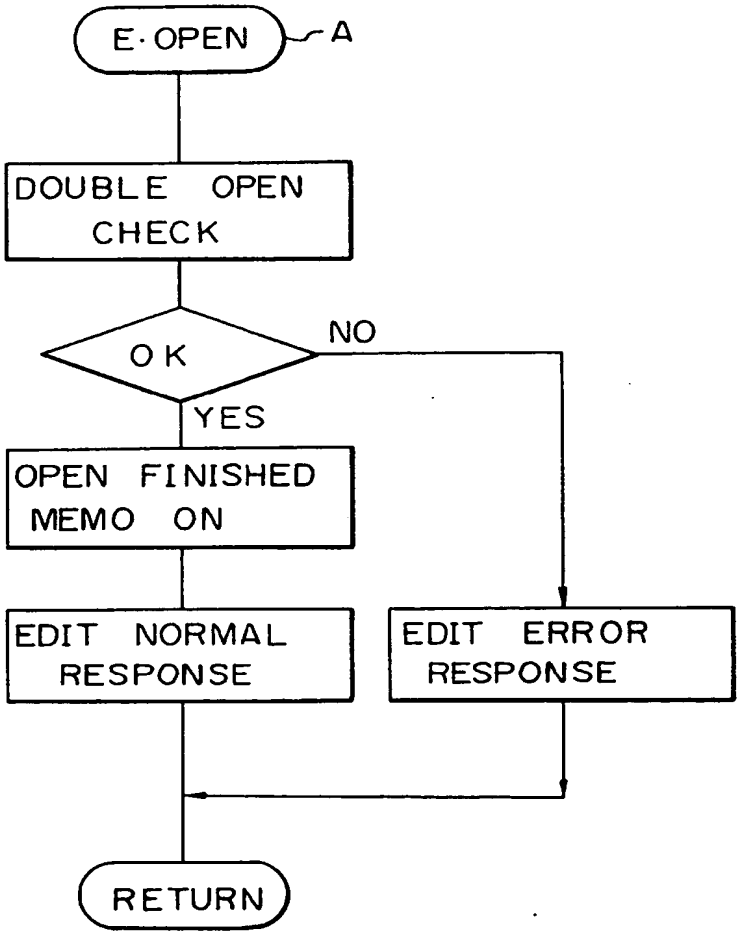

E·OPEN
A
DOUBLE OPEN CHECK
OK
NO
YES
OPEN FINISHED MEMO ON
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 13

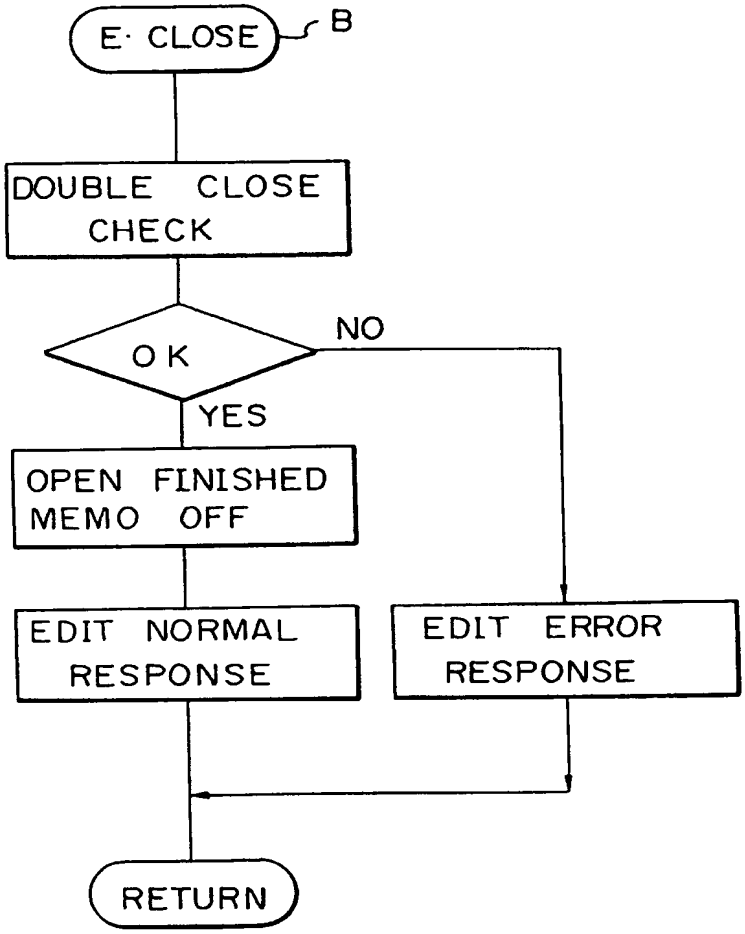

E· CLOSE
B
DOUBLE CLOSE CHECK
O K
NO
YES
OPEN FINISHED MEMO OFF
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 14

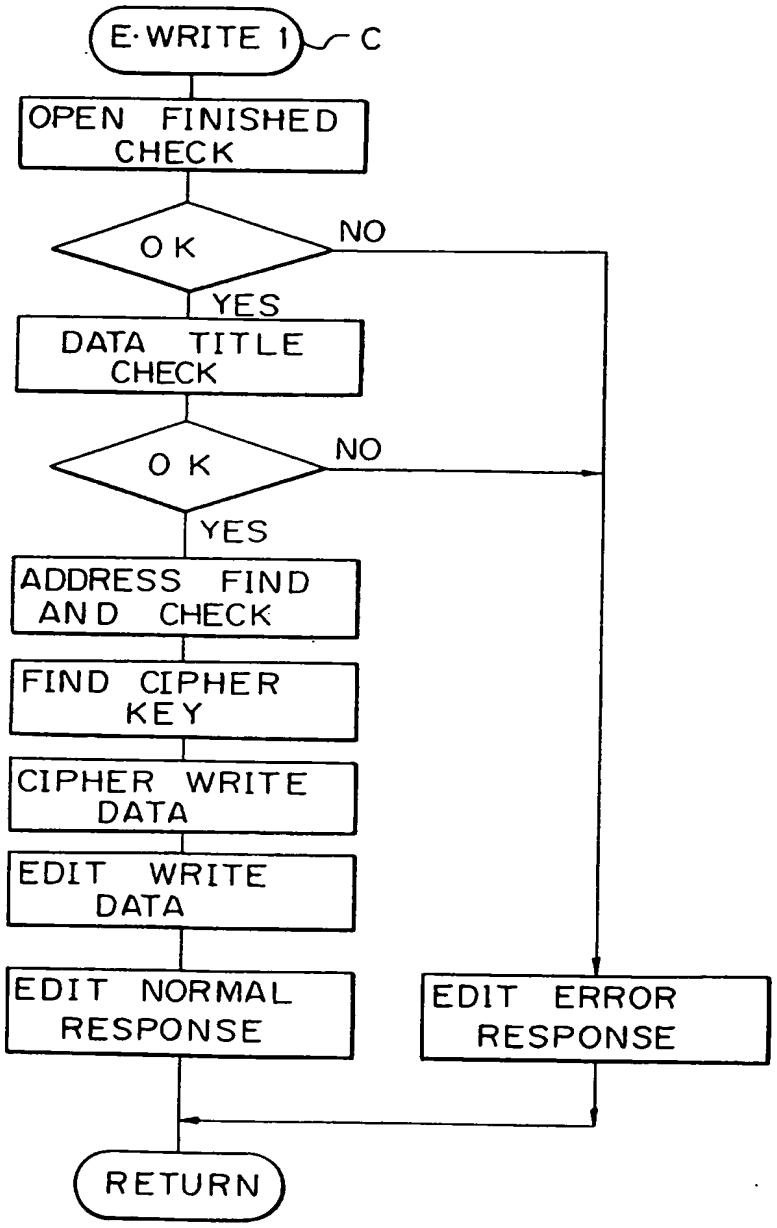

E·WRITE 1
C
OPEN FINISHED CHECK
O K
NO
YES
DATA TITLE CHECK
O K
NO
YES
ADDRESS FIND AND CHECK
FIND CIPHER KEY
CIPHER WRITE DATA
EDIT WRITE DATA
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 15

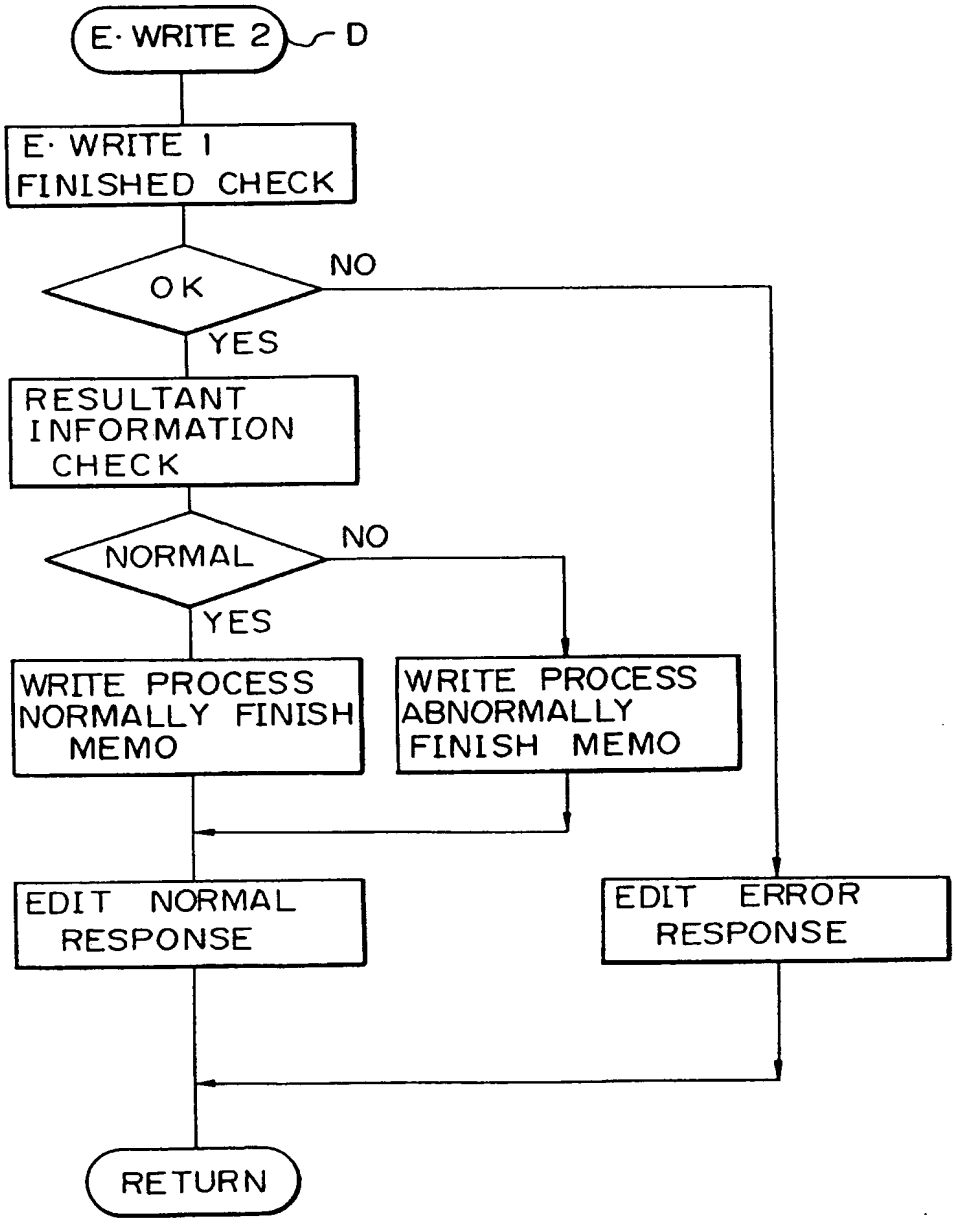

E·WRITE 2
D
E·WRITE 1 FINISHED CHECK
OK
NO
YES
RESULTANT INFORMATION CHECK
NORMAL
NO
YES
WRITE PROCESS NORMALLY FINISH MEMO
WRITE PROCESS ABNORMALLY FINISH MEMO
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 16

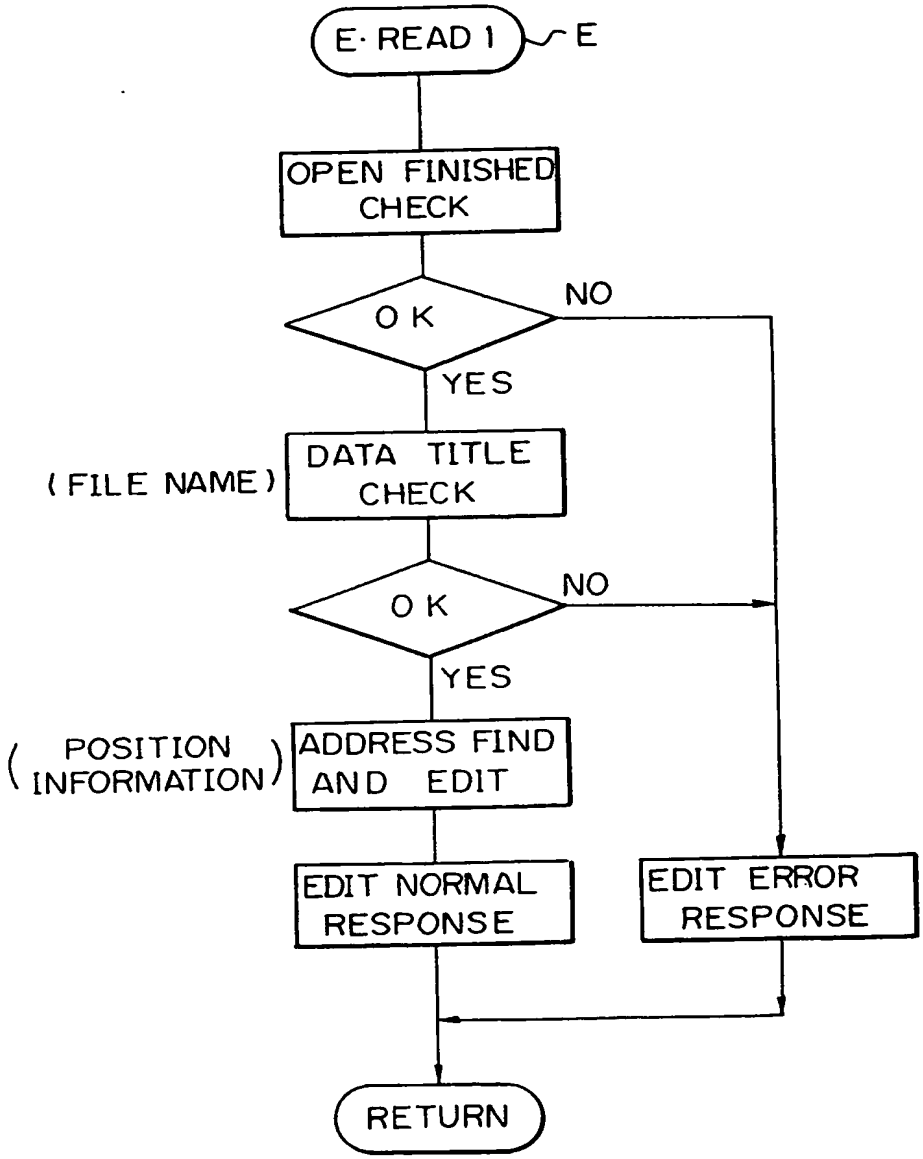

E·READ 1
E
OPEN FINISHED CHECK
O K
NO
YES
(FILE NAME)
DATA TITLE CHECK
O K
NO
YES
(POSITION INFORMATION)
ADDRESS FIND AND EDIT
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 17

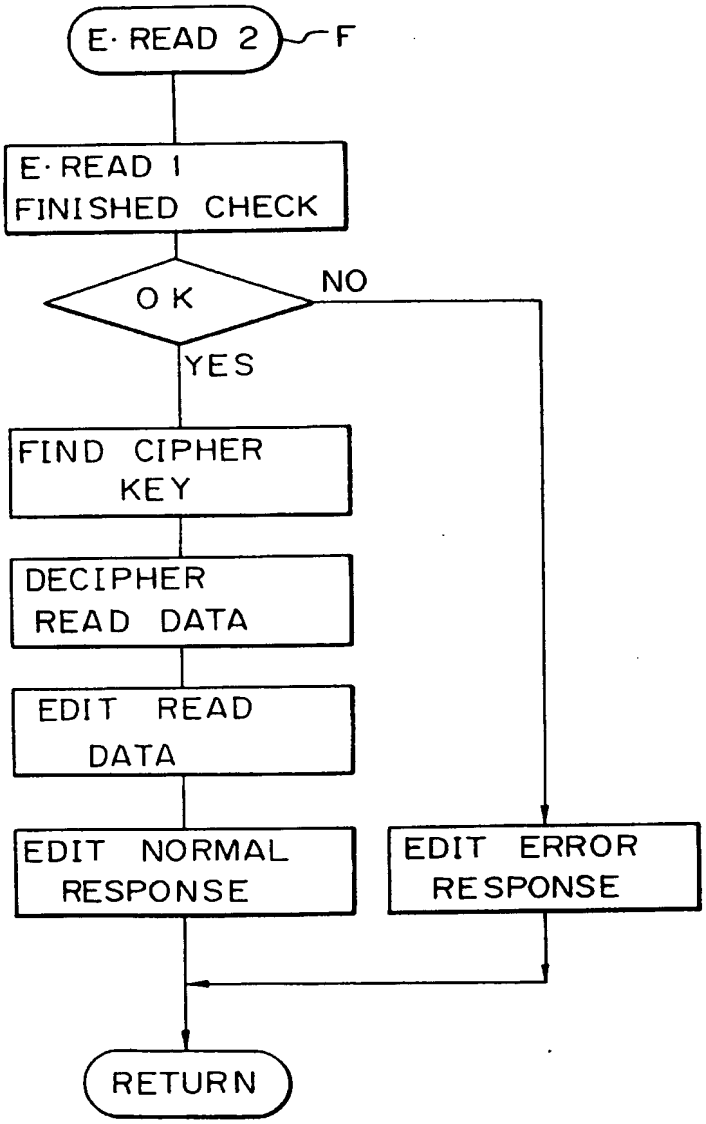

E·READ 2
F
E·READ 1
FINISHED CHECK
O K
NO
YES
FIND CIPHER
KEY
DECIPHER
READ DATA
EDIT READ
DATA
EDIT NORMAL
RESPONSE
EDIT ERROR
RESPONSE
RETURN

Fig. 18

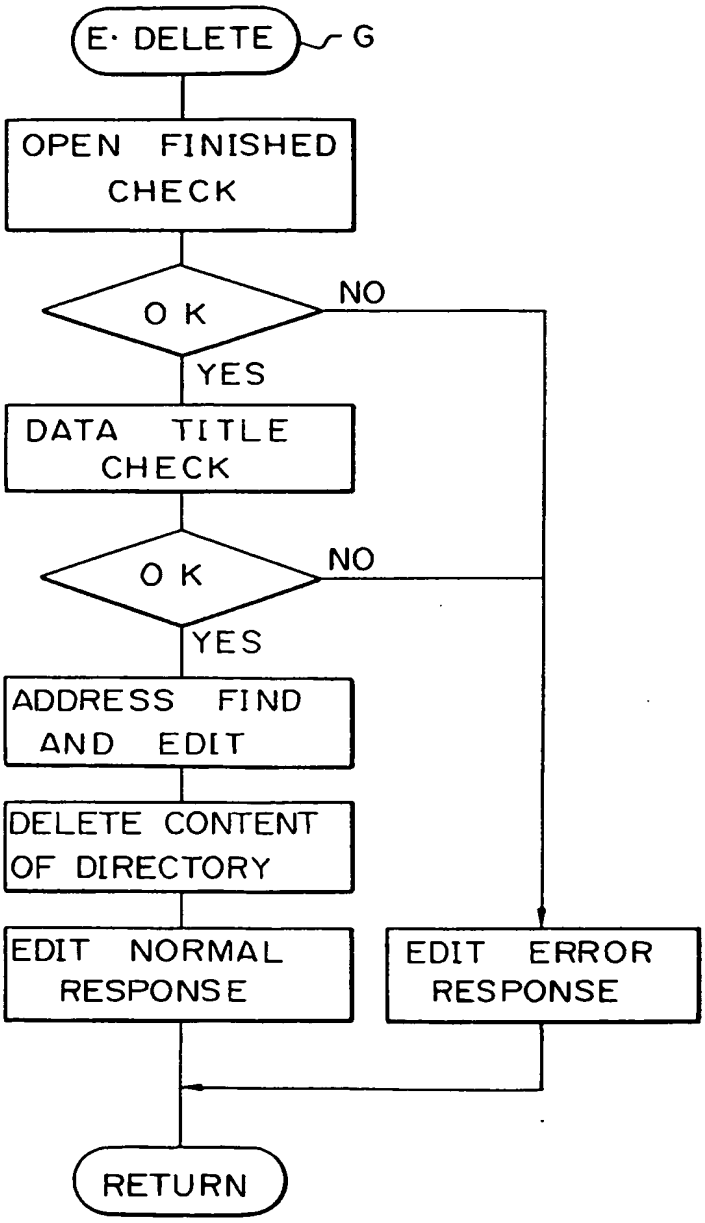

E· DELETE
G
OPEN FINISHED CHECK
O K
NO
YES
DATA TITLE CHECK
O K
NO
YES
ADDRESS FIND AND EDIT
DELETE CONTENT OF DIRECTORY
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 19

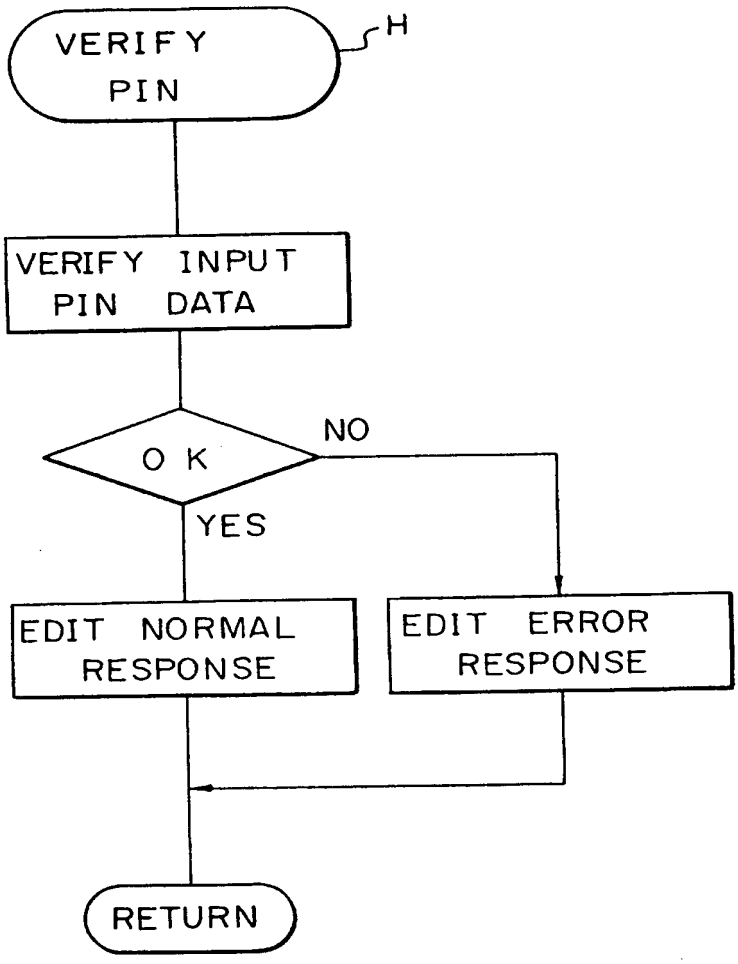

VERIFY PIN
H
VERIFY INPUT PIN DATA
O K
NO
YES
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 20

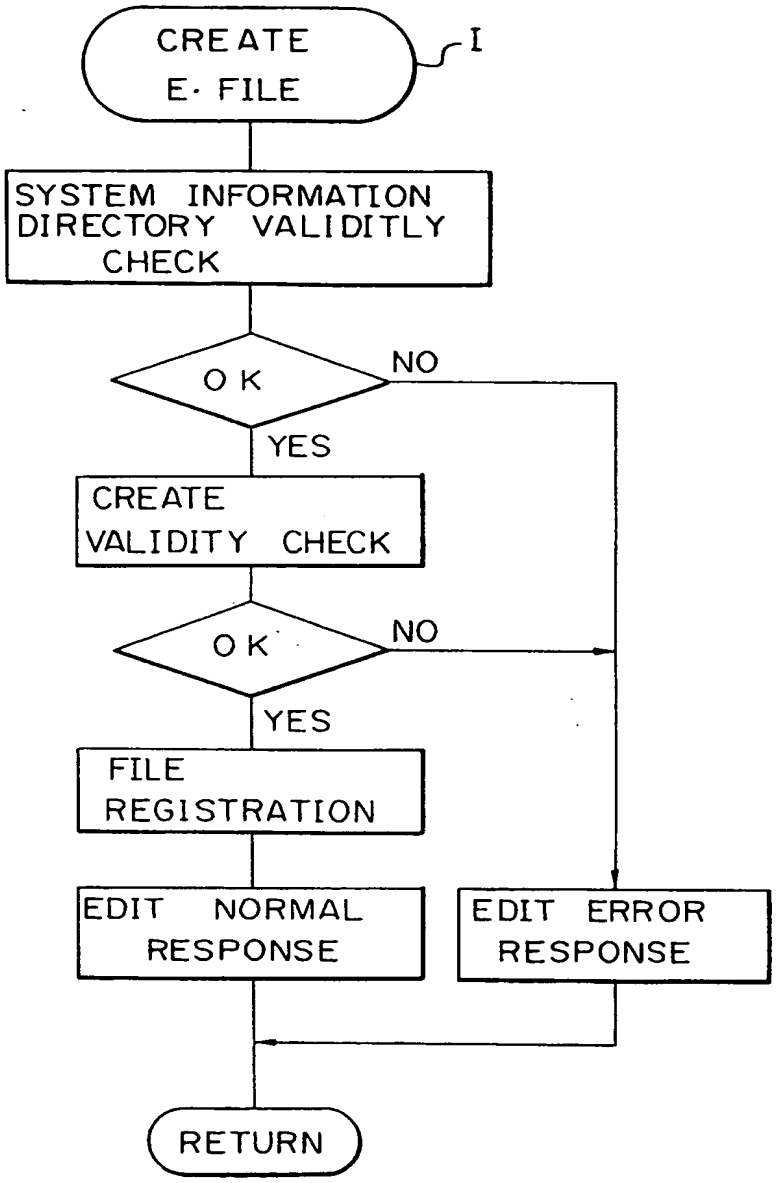

CREATE
E· FILE
I
SYSTEM INFORMATION
DIRECTORY VALIDITLY
CHECK
O K
NO
YES
CREATE
VALIDITY CHECK
O K
NO
YES
FILE
REGISTRATION
EDIT NORMAL
RESPONSE
EDIT ERROR
RESPONSE
RETURN

Fig. 21

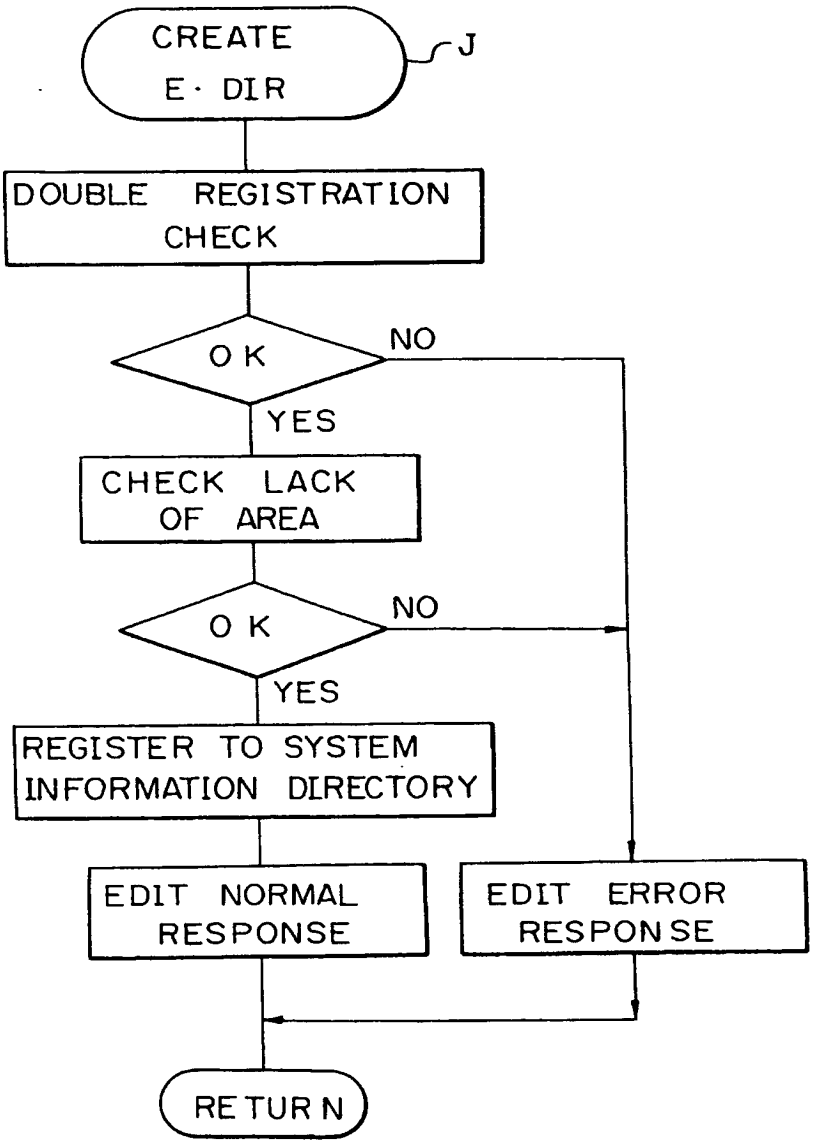

CREATE
E · DIR
J
DOUBLE REGISTRATION CHECK
O K
NO
YES
CHECK LACK OF AREA
O K
NO
YES
REGISTER TO SYSTEM INFORMATION DIRECTORY
EDIT NORMAL RESPONSE
EDIT ERROR RESPONSE
RETURN

Fig. 22

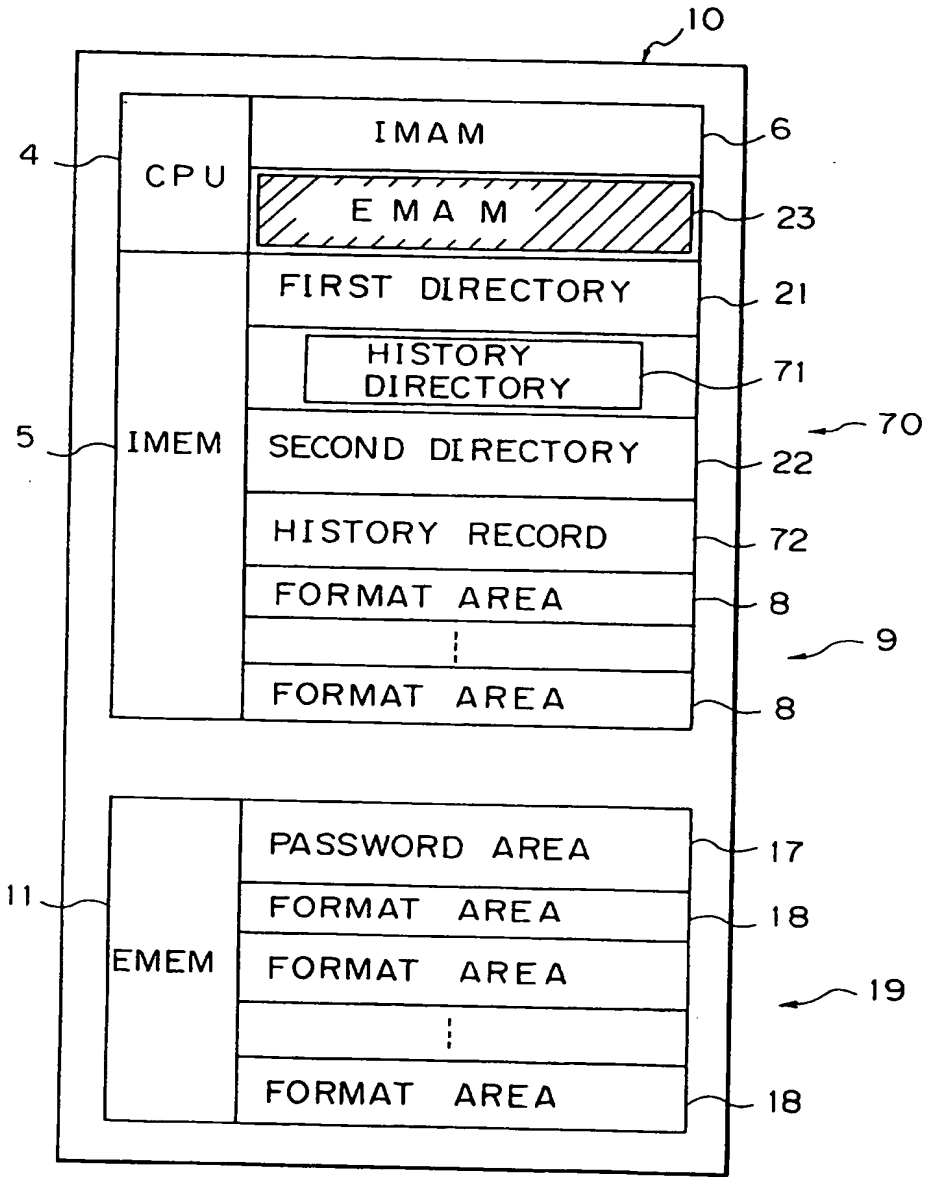

10
4
CPU
IMAM
6
EMAM
23
FIRST DIRECTORY
21
HISTORY DIRECTORY
71
70
5
IMEM
SECOND DIRECTORY
22
HISTORY RECORD
72
FORMAT AREA
8
9
FORMAT AREA
8
11
EMEM
PASSWORD AREA
17
FORMAT AREA
18
FORMAT AREA
19
FORMAT AREA
18

Fig. 23 A

Fig. 23

Fig. 23A	Fig. 23B

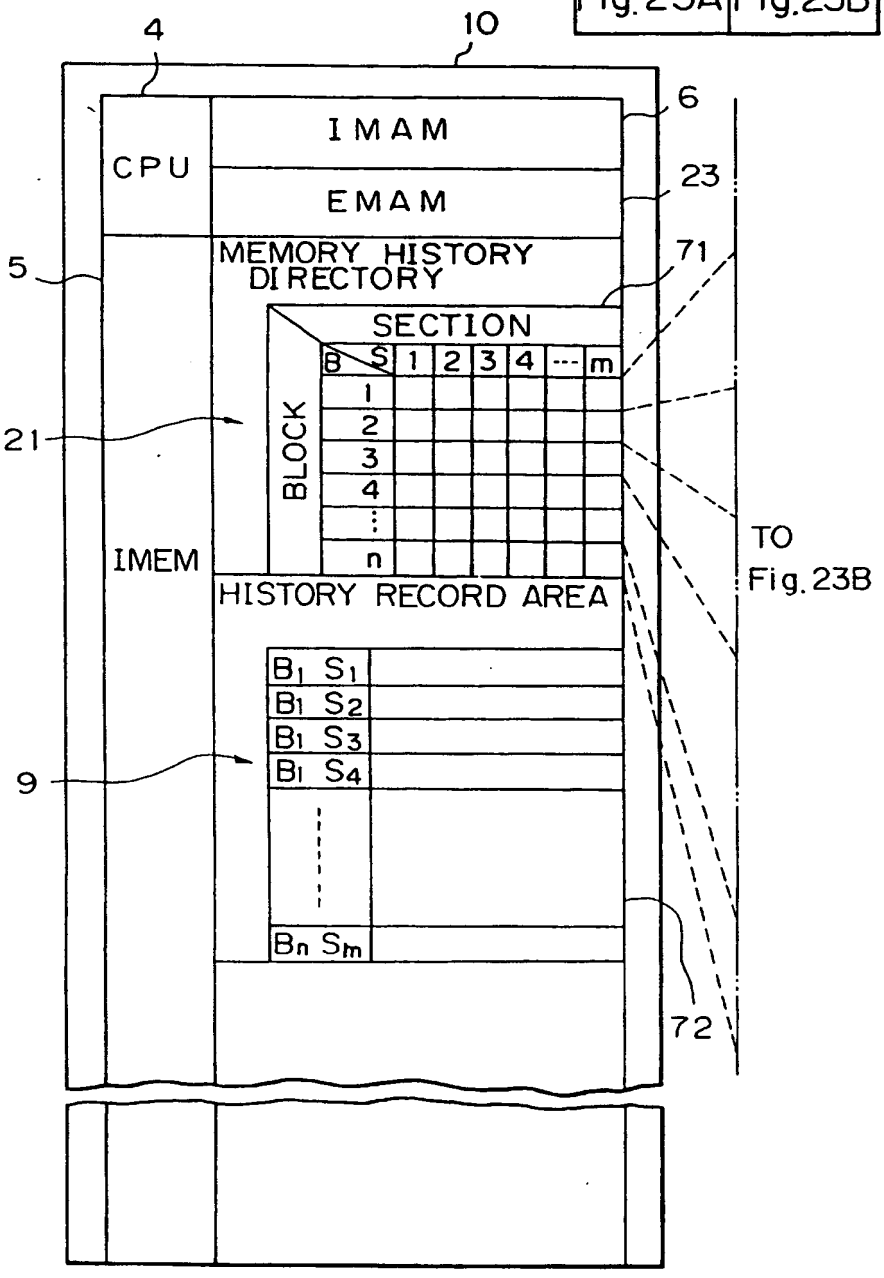


Fig. 23B

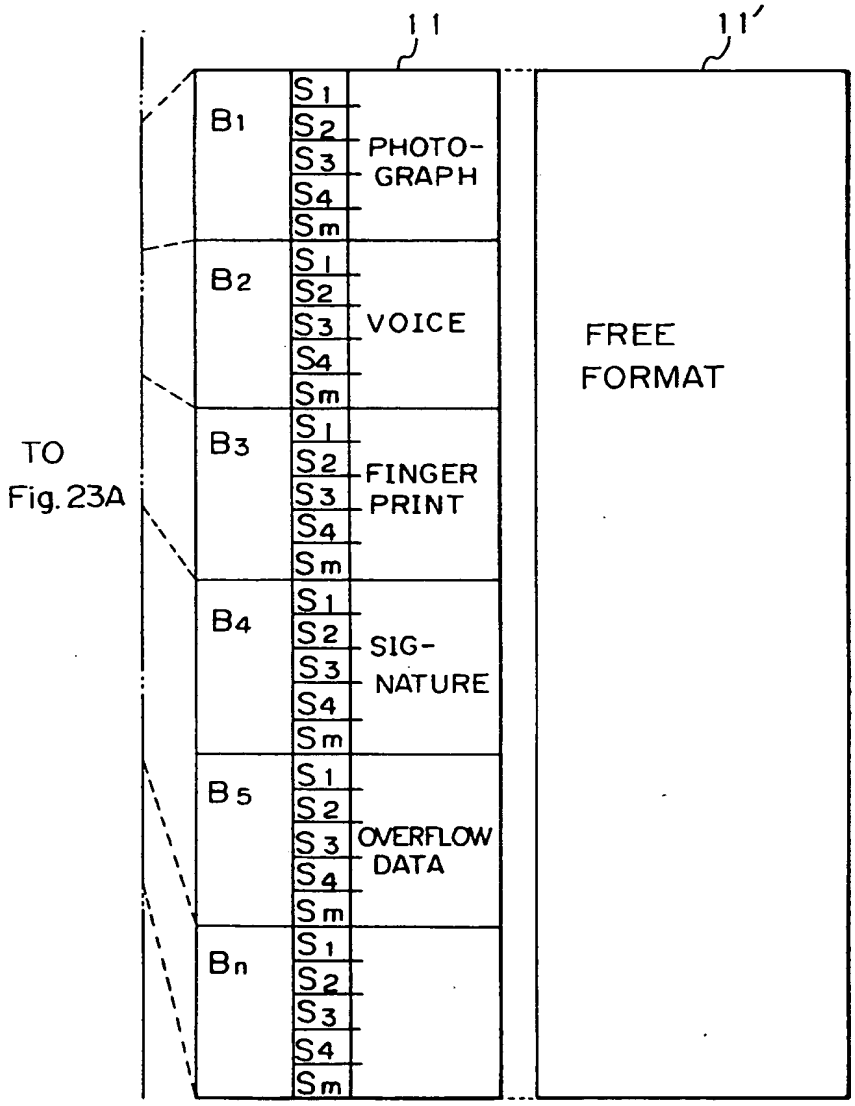

11
11'
B1
B2
B3
B4
B5
Bn
S1
S2
S3
S4
Sm
PHOTO-GRAPH
VOICE
FINGER PRINT
SIG-NATURE
OVERFLOW DATA
FREE FORMAT
TO Fig. 23A

Fig. 24A

Fig. 24

Fig. 24A	Fig. 24B

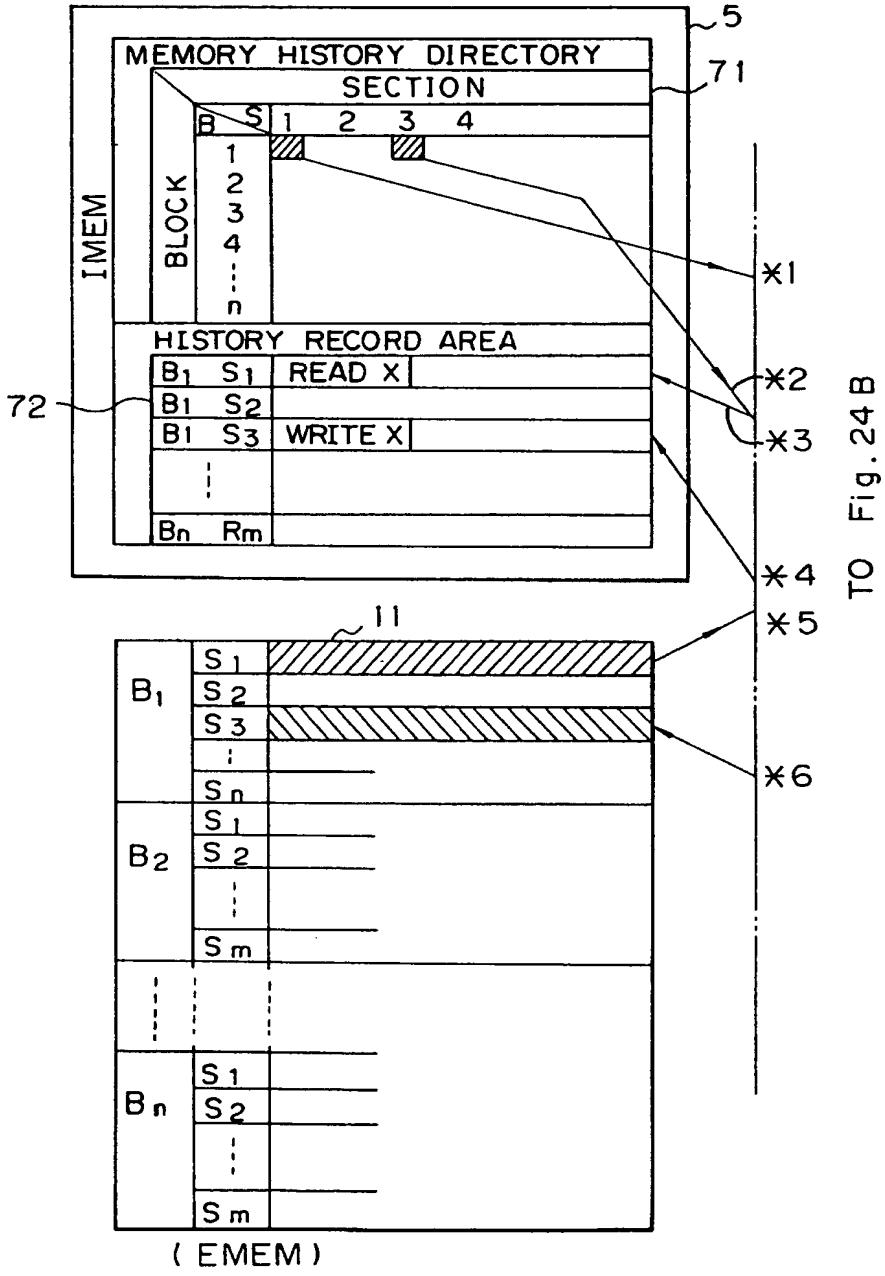
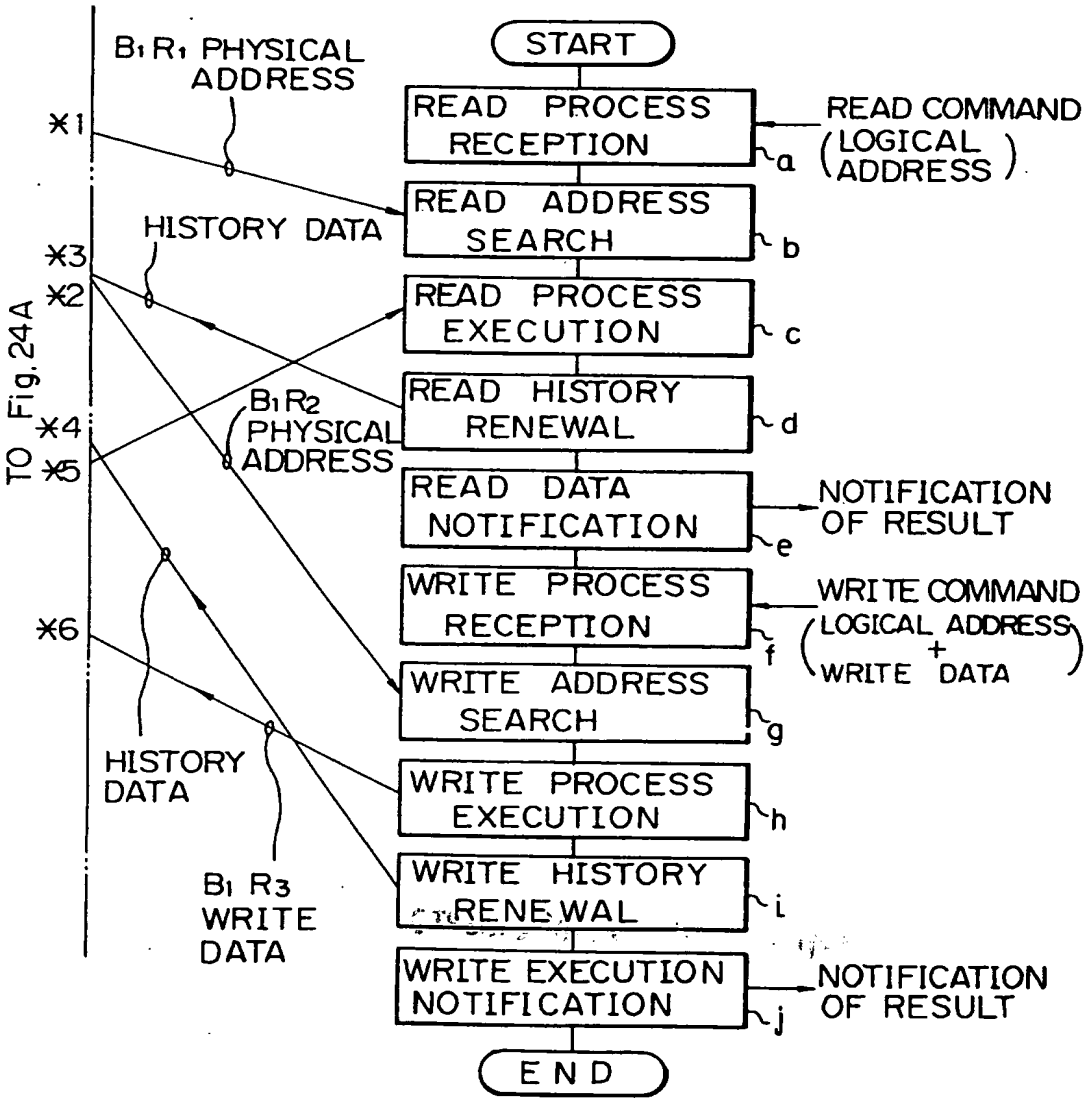


Fig. 24 B


START
READ PROCESS RECEPTION
a
READ COMMAND (LOGICAL ADDRESS)
READ ADDRESS SEARCH
b
READ PROCESS EXECUTION
c
READ HISTORY RENEWAL
d
READ DATA NOTIFICATION
e
NOTIFICATION OF RESULT
WRITE PROCESS RECEPTION
f
WRITE COMMAND (LOGICAL ADDRESS + WRITE DATA)
WRITE ADDRESS SEARCH
g
WRITE PROCESS EXECUTION
h
WRITE HISTORY RENEWAL
i
WRITE EXECUTION NOTIFICATION
j
NOTIFICATION OF RESULT
END
B1 R1 PHYSICAL ADDRESS
HISTORY DATA
B1 R2 PHYSICAL ADDRESS
HISTORY DATA
B1 R3 WRITE DATA
*1
*2
*3
*4
*5
*6
TO Fig. 24A